
**Universidad Nacional Mayor de San Marcos**

**Universidad del Perú. Decana de América**

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas


# Análisis de riesgos en seguridad informática caso UNMSM

**TESINA**

Para optar el Título Profesional de Ingeniero de Sistemas


**AUTOR**

Regina Magie SÁNCHEZ SÁNCHEZ

**ASESOR**

Jorge Santiago PANTOJA COLLANTES



Lima, Perú

2007

**Referencia bibliográfica**

Sánchez, R. (2007). *Análisis de riesgos en seguridad informática caso UNMSM*. Tesina para optar el título de Ingeniero de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

**INDICE**

CAPITULO III

3. MARCO TEORICO CONCEPTUAL

## RESUMEN

## ANÁLISIS DE RIESGOS EN SEGURIDAD INFORMÁTICA: CASO UNMSM

Regina Magie Sánchez Sánchez

Septiembre – 2007

**Asesor : Jorge Pantoja Collantes**

**Grado : Tesina Título**

El presente trabajo tiene como objetivo realizar un Análisis de Riesgos en Seguridad Informática en la UNMSM, lo cual permitirá desarrollar procesos y procedimientos seguros basados en políticas y estándares recomendados por el estado peruano (ONGEI - Oficina Nacional de Gobierno Electrónico e Informática) y el ISO 17799 (BS 7799-1), completo conjunto de controles, internacionalmente reconocidos, que abarcan las mejores prácticas en materia de seguridad de la información.

Se seguirá el modelo de procesos de cuatro fases PDCA (Plan – Do – Check - Act): Planificar, Hacer, Verificar y Actuar, que trata del establecimiento, implementación y operación, monitoreo y mejoramiento continuo del sistema de gestión de seguridad informática, y el cual esta definido en el estándar BS 7799-2. El resultado de estas estrategias hace que la estructura del Sistema de Gestión de Seguridad Informática conforme el paradigma de gestión de riesgos a partir del esquema de controles definidos en la ISO 17799, más el dinamismo propio del modelo PDCA.

La realización de este documento pretende ayudar a entender que el establecimiento de un Sistema de Gestión de Seguridad Informática en la institución es de vital importancia. El desarrollo de este tipo de proyectos mejora de forma rápida y efectiva los niveles de calidad en la prestación de los servicios de tecnología ofrecidos por la organización a los usuarios tanto internos como externos, no solamente desde el punto de vista de mejora del rendimiento, sino también asegurando la información dedicando los recursos necesarios para lo que están planificados.

Para la consolidación de un Plan de Seguridad Informática es imprescindible que todos y cada uno de los miembros de la comunidad universitaria se involucren en el mismo, asignando roles y responsabilidades; en particular, debe contarse con un compromiso real de cumplimiento por parte de los órganos directivos ya que sin su apoyo poco o nada se va a lograr. Parte de ese apoyo debe reflejarse en un presupuesto económico adecuado para llevar a cabo el plan, asignando los recursos que sean necesarios.

**Palabras Clave:**

Análisis de riesgos, sistema de gestión de seguridad informática, plan de seguridad informática, estándar

## ABSTRACT

### ANÁLISIS DE RIESGOS EN SEGURIDAD INFORMÁTICA: CASO UNMSM

Regina Magie Sánchez Sánchez

Septiembre – 2007

**Adviser : Jorge Pantoja Collantes**

**Degree : Tesina Título**

The present document has the main objective of carry out a Risks Analysis in Information Security in the UNMSM, which will permit to develop secure processes and procedures based on politics and standards recommended by the Peruvian state (ONGEI - Oficina Nacional de Gobierno Electrónico e Informática) and the ISO 17799 (BS 7799-1), complete framework of controls, internationally recognized, that provides the best practices in information security.

It will continue the four phases PDCA process model (Plan – Do – Check - Act), that tries the establishment, implementation and operation, monitoring and continuous improvement of the information security management system, and which is defined in the BS 7799-2 standard. The result of these strategies does that the structure of the Information Security Management System in agreement with the risks management paradigm from the plan of defined controls in the ISO 17799, plus the own dynamism of the PDCA model.

The execution of this document intends to help to understand that the establishment of an Information Security Management System in the institution is of vital importance. The development of this kind of projects improve in a fast and effective way the quality levels in the installment of the services of technology offered by the organization to the internal and external users, not only since the point of view of improvement of the performance, but also assuring the information dedicating the necessary resources for what are planned.

For the consolidation of the Information Security Plan is indispensable that all and each one of the members of the university community get involved in the same one, assigning roles and responsibilities; particularly, should include a real commitment of compliance on the part of the executive staff since without its support little or nothing is going to achieve. Part of that support should be reflected in an adequate economic budget to carry out the plan, assigning the adequate resources.

**Keywords:**

Risk analysis, information security management system, information security plan, standard

# INTRODUCCIÓN

El término seguridad posee múltiples significados según el ambiente donde se emplee, lo cual lo convierte en un término ambiguo, amplio e impreciso. En sentido general puede entenderse como aquellas técnicas y/o actividades destinadas a la prevención, protección y salvaguarda de todo aquello que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal u organizacional.

Si tenemos en cuenta su sentido referido puramente a la informática podemos definirla como el conjunto de reglas, planes y acciones que permiten garantizar la prestación de servicios y asegurar la información contenida en un sistema de cómputo. En este sentido, la información es el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales. El origen de las amenazas informáticas a las que hacer frente es muy variado; desde fenómenos naturales hasta artificiales como un accidente, espionaje industrial, sabotaje, virus informáticos, ataques o piratería electrónica.

Hoy en día, la seguridad informática ha adquirido un gran auge dadas las condiciones cambiantes de las nuevas plataformas y herramientas de computación existentes. Esta situación desemboca en la aparición continua de nuevas amenazas y vulnerabilidades que afectan a los sistemas informáticos. En particular, la posibilidad de interconectarse a través de redes ha abierto nuevos y amplios horizontes a las empresas para mejorar su productividad y poder explorar mas allá de sus fronteras, lo cual paralelamente ha traído

consigo la aparición de nuevos e importantes riesgos para el sistema de información de las organizaciones a los cuales es preciso hacer frente.

Para gestionar debidamente la seguridad informática dentro de una institución y hacer frente a las amenazas anteriormente citadas es preciso disponer de un buen Plan de Seguridad Informática. En él se definen el planteamiento, diseño e implantación de un modelo de seguridad con el objetivo de establecer una *cultura de la seguridad* (concientización) en toda la institución. Esto la obliga a redactar sus propios procedimientos de seguridad, los cuales han de estar enmarcados por las políticas que conforman este plan. El propósito de su establecimiento es la protección de la información y los activos de la institución, tratando de conseguir la confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que deben asumir todos y cada uno de los empleados de la institución, ya que, en última instancia, depende de todos y cada uno de ellos, por lo que es esencial que se integre en su quehacer diario.

De esta manera, las políticas de seguridad informática surgen como una herramienta mediante la cual se pretende concientizar a los miembros de una institución acerca de la importancia y la sensibilidad de la información y de los servicios críticos que permiten a la organización desarrollarse y mantenerse en su sector de negocios, fijando los mecanismos y procedimientos que las empresas deben adoptar para salvaguardar sus sistemas y la información que estos contienen.

El objetivo fundamental de la seguridad informática no es la protección de los sistemas, sino la *reducción de los riesgos* y el soporte a las operaciones del negocio para lo cual ha de cubrir los siguientes campos: la seguridad de las personas, de la información, de las comunicaciones y de los sistemas. Para ser efectiva, la seguridad debe estar integrada en los procesos de la empresa y no estar relegada meramente a ciertas aplicaciones técnicas.

Se debe hacer constar que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos. Ninguno es fiable al cien por cien. Debido a esto es necesario estar preparado y dispuesto a reaccionar con rapidez ante cualquier eventualidad imprevista, ya que, como se ha indicado anteriormente, las amenazas a las que es preciso hacer frente y las vulnerabilidades potenciales a tener en cuenta están cambiando constantemente.

# CAPÍTULO I

# 1. PLANTEAMIENTO DEL PROBLEMA

## 1.1 Fundamentación del Problema

### 1.1.1 Descripción de la Realidad

La Universidad, hoy está experimentando cambios en extremo turbulentos que han movido su base de sustento de un ambiente de negocio tradicional y concentrado de recursos humanos, tecnológicos, financieros y académicos, a uno donde la descentralización ha llegado a los límites de la virtualidad.

En tal sentido, la Universidad ha venido implementado, a lo largo de este tiempo, varios servicios que permiten a la comunidad universitaria realizar sus trámites de una manera ágil sin la necesidad de apersonarse al campus. Esto nos hace pensar en la importancia de velar y asegurar la disponibilidad de estos servicios, y el problema que ocasionaría a los usuarios el no contar con estos.

Frente al crecimiento del numero de servicios ofrecidos, se define claramente una necesidad de ampliar y definir los límites de la cobertura en cuanto a un tema importante, que en la mayoría de casos es obviado,

pero en realidad debería de ser uno de los más importantes, como lo es la seguridad informática.

Algunas organizaciones, por lo general las del sector público, e incluso algunas de desarrollo de software, presentan un desinterés en cuanto a la inversión, concientización e información sobre la seguridad de su información digital, o sobre la implementación de un área de seguridad informática; es mas, están bastante desinformados que no ven la necesidad de proteger la información contenida en sus equipos de computo, en el peor de los casos que estas se encuentren conectadas a Internet sin un nivel adecuado de protección, ya que sólo atinan con instalar un antivirus como única medida de seguridad necesaria y suficiente.

Un punto en contra de la implementación de soluciones de seguridad es la inversión; como es lógico, en la medida que se requiera un sistema más seguro se tendrá que contemplar una inversión económica mayor. Con respecto a esta cuestión es necesario decir que, en general, las organizaciones son bastante reticentes a destinar grandes cantidades de fondos a la seguridad informática ya que estos no repercuten en un aumento de la productividad (y consiguientemente de los beneficios) que, al fin y al cabo, constituye el interés primero de la empresa.

Por cuestión de costos, se prefieren soluciones de software de seguridad en versiones de prueba o de adquisición ilegal, algo natural en nuestro ambiente. Este último cumple con su labor pero pone en riesgo la

información de la empresa, debido a que ha sido manipulado, y por ello no brinda ninguna garantía. Al momento de sufrir una grave eventualidad será cuando la empresa tome conciencia de la importancia de la adquisición de una solución de seguridad.

Como se mencionó con anterioridad, la Universidad ha tomado medidas al respecto adquiriendo sistemas de seguridad para salvaguardar la información que en ella se generan de diferente índole, como por ejemplo; financiero, de investigación, de conocimientos, de transacciones administrativas diarias, del sistema de correo electrónico, de la base de datos principal, etc., mediante equipos antivirus para proteger los correos, software antivirus para los computadores de escritorio, software de filtrado de contenido, cortafuego para proteger el perímetro de la LAN de la Universidad, y medidas de seguridad aplicadas en los diversos equipos servidores y las estaciones de trabajo.

El hecho de no contar con un sistema de seguridad integral, que implica a los sistemas de seguridad y la definición de un plan para la administración de estos, hace que aún se presenten los siguientes problemas:

- No se cuenta con un plan integrado de seguridad informática.
- La solución de eventualidades se realiza de acuerdo a la experiencia con la que cuenta el personal encargado.
- No se tiene definido y documentado un plan de contingencias para la solución de problemas.

- No se tiene definidas las responsabilidades de las personas pertenecientes al área de informática en el caso de suceder alguna eventualidad.
- Falta de concientización de los usuarios ante las consecuencias del mal uso de los activos informáticos que se encuentran a su cargo.
- Falta de visión a nivel estratégico de contar con un plan de seguridad de la información.
- El recorte presupuestal que limita la implementación de proyectos en el área de seguridad informática.
- Falta de especialización del personal responsable sobre su área, a nivel de todo personal informático.
- Falta de auditoria informática.
- El 75% del personal de informática de las dependencias no cuenta con el perfil profesional requerido.
- Resolución de problemas en forma aislada.
- No se tiene definido el nivel de acceso a la información.
- Sustracción de información utilizando medios de almacenamiento de gran capacidad portátiles y de reducido tamaño

Este estudio pretende investigar los caminos que el área de informática responsable de la Universidad debe seguir, para formular una estrategia para el desarrollo, adquisición y aplicación de los elementos de seguridad. Esto implica implementar estrategias orientadas a la concientización de la comunidad universitaria del riesgo de tener su información en un dispositivo digital, como por ejemplo: una máquina

conectada o NO a Internet, los diferentes dispositivos de almacenamiento (memorias USB, disquetes, CD, DVD, etc.), buscando el apoyo de los distintos organismos o grupos que conforman la Universidad, lo que producirá una mejor competitividad de la institución en el mercado de la educación universitaria manteniendo su información disponible, confiable e integra. ***El objetivo de este proyecto de tesina es realizar un Análisis de Riesgos que dará inicio a la elaboración del plan de seguridad informática para la gestión y resguardo de la información.***

### 1.1.2 Antecedentes del Problema

**Evolución del Código Malicioso**

Lejos quedan ya los tiempos en los que los creadores de malware buscaban afán de protagonismo, notoriedad y reconocimiento a través de sus creaciones. El conocimiento o know-how de este colectivo se utiliza hoy en día con fines lucrativos.

Cada vez existe mayor acceso a la información necesaria para desarrollar malware. En esta línea cabe destacar la publicación del código fuente de ciertas familias de malware, bajo círculos underground e incluso, en algunos casos, a través de redes P2P (peer-to-peer) accesibles al público en general. A esta circunstancia hay que añadir la cada vez más agresiva política de publicación de exploits dirigidos contra vulnerabilidades conocidas, en ocasiones sin estar aún disponible los correspondientes parches. La disponibilidad de herramientas adecuadas

facilita la vida a aquellos que se planteen la posibilidad de desarrollar un espécimen de malware. Este punto representa precisamente el nexo de unión con la criminalización del malware: una actividad al margen de la ley como esta, incentivada de forma lucrativa, y facilitada mediante la disponibilidad de herramientas adecuadas, tiene ya una buena parte del camino recorrido para convertirse en un serio problema.

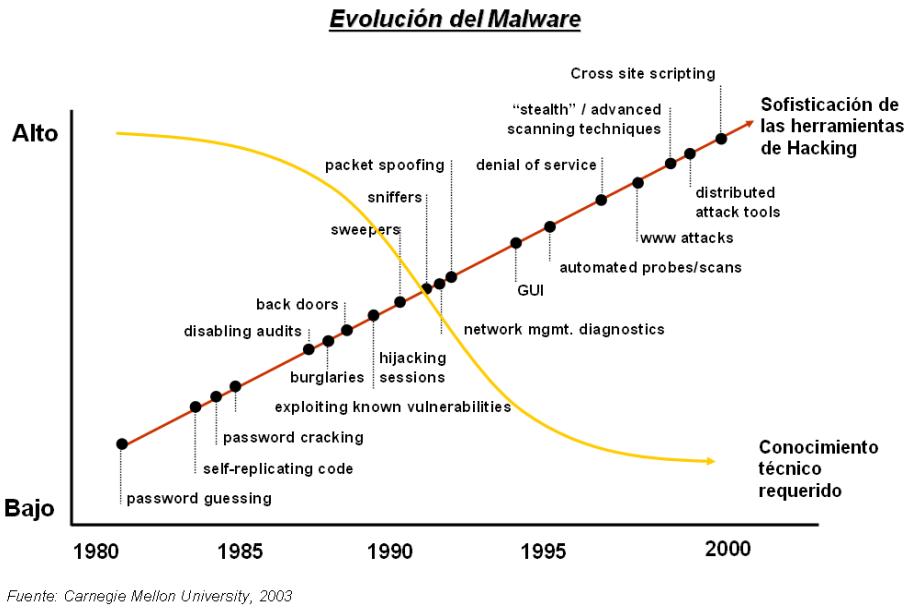



**Grafico Nº 1 – Sofisticación de las Herramientas de Hacking**

Los acontecimientos de los dos últimos años en materia de malware, han evidenciado de forma rotunda las debilidades de las tecnologías antimalware que se han venido utilizando hasta el día de hoy. Se puede concluir, casi de forma irrefutable, que dichas tecnologías no son suficientes en si mismas para lograr parar una avalancha de malware de semejantes proporciones. Algunas de las tecnologías actuales, empleadas de forma conjunta y coordinada, permiten mitigar esta clase de plagas, pero en ningún caso ajustándose a un coste total de propiedad adecuado. Se necesitan, por tanto, nuevas tecnologías

capaces de cubrir el vacío dejado por las actuales y, al mismo tiempo, nuevas formas de integrar todas ellas manteniendo un coste total de propiedad razonable.

## Análisis Estadístico a Nivel Internacional del Problema

### Análisis de Vulnerabilidades

Según la publicación IBM Internet Security Systems X-Force® 2006 Trend Statistics, de Enero del 2007, el aumento exponencial de las vulnerabilidades en el 2006 más que en todos los años anteriores rompió los récords. Con 7,247 vulnerabilidades descubiertas en el 2006, el conteo total de vulnerabilidades aumentó casi 40% sobre el año anterior. Desde el inicio del nuevo milenio, ha habido un aumento del 261% en vulnerabilidades, un promedio de 23% al año. Esta tendencia sigue a lo largo del presente año. El incremento de vulnerabilidades año a año se puede observar en el siguiente grafico:


| Año | Vulnerabilidades | Prom por mes | Prom por semana | % incremento año sobre año |
|---|---|---|---|---|
| 2000 | 2007 | 167 | 39 | |
| 2001 | 1918 | 160 | 37 | -4.4% |
| 2002 | 3210 | 268 | 62 | 67.4% |
| 2003 | 3156 | 263 | 61 | -1.7% |
| 2004 | 4606 | 384 | 89 | 45.9% |
| 2005 | 5195 | 433 | 100 | 12.8% |
| 2006 | 7247 | 604 | 139 | 39.5% |

*Fuente: IBM Internet Security Systems X-Force® 2006 Trend Statistics*

**Grafico Nº 2**

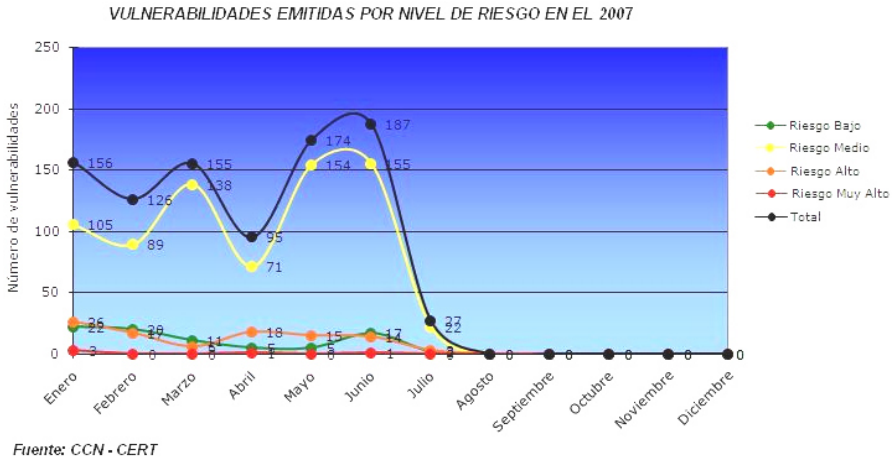
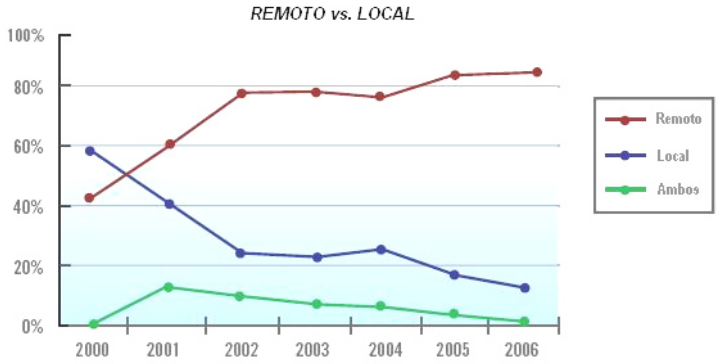



**Grafico Nº 3**

## Explotación de Vulnerabilidades Remotas vs. Locales

En un mundo de la explotación de vulnerabilidades, las más apreciadas de las vulnerabilidades son las que pueden ser explotadas remotamente. En el 2006, el porcentaje de vulnerabilidades remotamente explotables alcanzó un punto alto nunca igualado del 88,4%.

En el gráfico siguiente, "Remoto" representa vulnerabilidades que pueden ser explotadas a través de una red. "Local" representa vulnerabilidades que sólo pueden ser explotadas después de accesar a un equipo local o desde un equipo de escritorio. Y "Ambos" representa vulnerabilidades que pueden ser explotadas remotamente y localmente. Para los fines del gráfico a continuación, "Ambos" es una subcategoría asumida del total de "Remoto".




| Año | % de Vulnerabilidades Remotas | % de Vulnerabilidades Locales |
|---|---|---|
| 2000 | 43.6% | 56.4% |
| 2001 | 57.4% | 42.6% |
| 2002 | 75.7% | 24.3% |
| 2003 | 76.6% | 23.4% |
| 2004 | 73.3% | 26.7% |
| 2005 | 84.8% | 15.2% |
| 2006 | 88.4% | 11.6% |

*Fuente: IBM Internet Security Systems X-Force® 2006 Trend Statistics*

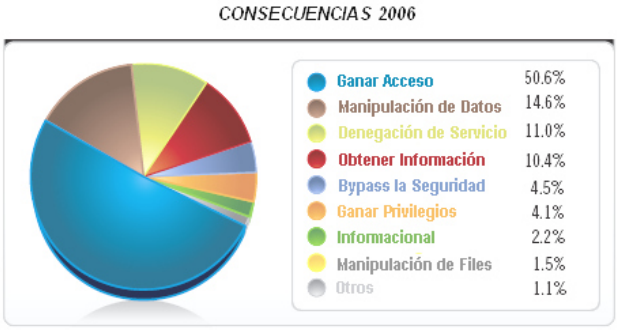
**Grafico Nº 4**

Al comparar el número de vulnerabilidades que pueden ser explotadas por un atacante remoto versus aquellas que pueden ser explotadas por un atacante local, se observó una tendencia alarmante que se ha estado desarrollando desde el año 2000. En el 2000, sólo el 43,6% de todas las vulnerabilidades descubiertas fueron explotadas remotamente. El número de vulnerabilidades que pueden ser explotadas remotamente ha continuado creciendo cada año, alcanzando su punto más alto en el 2006.

## Consecuencias de la Explotación de las Vulnerabilidades

Como parte de la investigación en cada vulnerabilidad descubierta en el 2006, se registran las consecuencias principales de la explotación. Las consecuencias están divididas en nueve categorías. En el 2006, la

consecuencia más común de la explotación fue "Ganar Acceso," que contabilizó el 50,6% de todas las vulnerabilidades.




*Fuente: IBM Internet Security Systems X-Force® 2006 Trend Statistics*

**Grafico Nº 5**

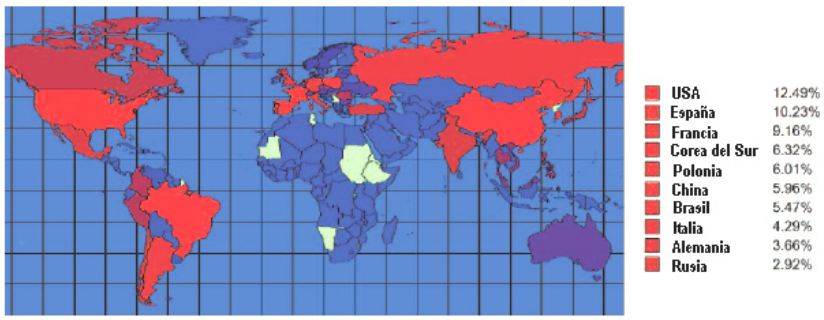
## Análisis de Spam

Dentro de los últimos 12 meses, el volumen de spam ha aumentado en un 100%. Consecuentemente, aunque los algoritmos de descubrimiento de spam y las tecnologías han mejorado a lo largo del año, a menudo parece que más correos electrónicos spam llegan al buzón del usuario y por lo tanto subjetivamente los usuarios "sienten" que la detección de spam no ha mejorado.

En un día promedio, IBM ISS analiza más de 150.000 mensajes de spam únicos – por lo cual, utilizando la tecnología fuzzy-fingerprint, un mensaje "único" de spam es aquel que es por lo menos 10% diferente a cualquier otro mensaje de spam anteriormente recibido. La tecnología que IBM utiliza, mira pasar las tentativas de engaño de un mensaje y genera un fuzzy-fingerprint (huella) por cada uno identificado como spam. Una huella entonces es generada para cada mensaje de correo

electrónico en los buzones de los usuarios y, si las huellas coinciden, un mensaje de spam es detectado.

*DISTRIBUCION DE LOS ENVIADORES DE SPAM*




*Fuente: IBM Internet Security Systems X-Force® 2006 Trend Statistics*

**Grafico Nº 6**

## Análisis de Malcode

El 2006 fue un gran año para el malware, con nuevos registros en volumen y sofisticación ocurriendo de manera mensual. Se identificaron, estudiaron y analizaron más de 200.000 nuevas muestras de malware a lo largo del año.

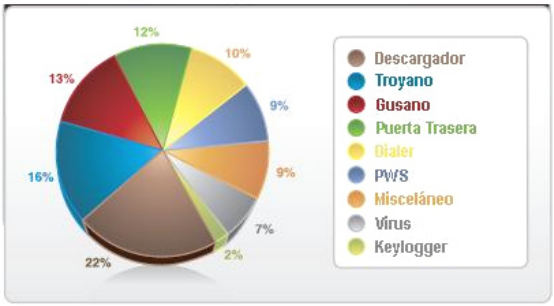
Una tendencia importante observada durante el 2006 fue la manera como el malcode continuó siendo menos claro en su categorización. El malcode continuó absorbiendo o prestando nuevas tecnologías para ser utilizadas por otros malware exitosos. De tal modo que, los "paquetes" clásicos de virus, gusanos, spyware, puertas traseras, etc. son grandemente irrelevantes. El malware moderno es ahora el equivalente digital de la navaja suiza.

En vez de eso, la clasificación se debe hacer con respecto a la característica primaria o más dominante del malware.

## Categorización del Malcode

La muestra recolectada de malware durante el 2006 puede ser dividida en varias categorías clave. El gráfico siguiente indica que la clase más grande de malware fueron los gestores de descarga.

*CATEGORIZACIÓN DEL MALCODE 2006*




*Fuente: IBM Internet Security Systems X-Force® 2006 Trend Statistics*

**Grafico Nº 7**

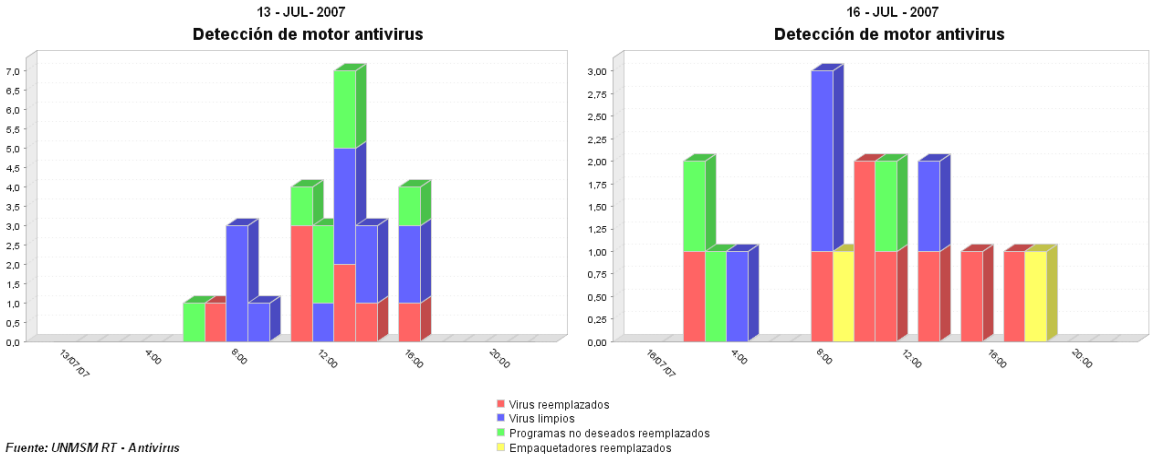
## Análisis Estadístico a Nivel Institucional del Problema

Hoy en día la Universidad no se encuentra exenta de ataques de hackers o curiosos, ser blanco de spammers, engaño (phishing), software espía (spyware), rootkits, troyanos, virus, gusanos, etc.; y debido a ello sus sistemas de seguridad son periódicamente actualizados o reemplazados por una nueva tecnología acorde al cambio dinámico y cada vez mas sofisticado del crimeware.

La Universidad cuenta con varios sistemas de seguridad perimetrales, entre ellos tenemos el Detector de Intrusos, Firewall, Antivirus, Anti-Spam, Anti-Phishing, Anti programas no deseados y el Administrador de Contenidos URL, con los que brinda protección a los recursos informáticos.

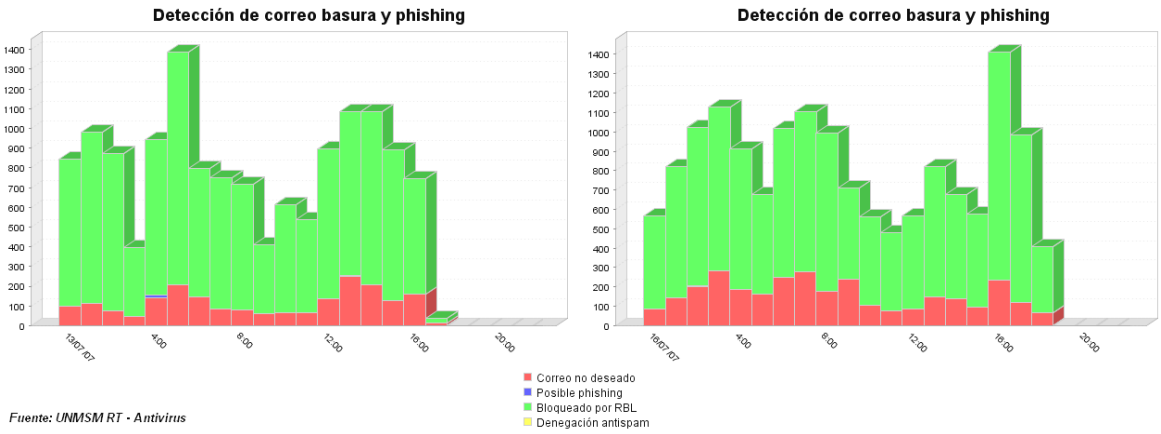
Los reportes elaborados por nuestros sistemas de seguridad corroboran el incremento de las incidencias que se han visto esquematizados en los gráficos anteriores.

En el siguiente gráfico se aprecia la detección del equipo de seguridad antivirus en un día ordinario:




*Fuente: UNMSM RT - Antivirus*

**Grafico Nº 8**




*Fuente: UNMSM RT - Antivirus*

**Grafico Nº 9**

El gráfico anterior muestra el tráfico de correo no deseado y phishing por hora durante un día. Se puede apreciar que gran cantidad de correo no deseado ha sido bloqueado por encontrarse registrado en listas negras

RBL, el cual constituye una base de datos de equipos en Internet que envían correos masivos a todo el mundo.

En este gráfico se muestran en detalle los códigos maliciosos que atacan directamente al servidor de correo.

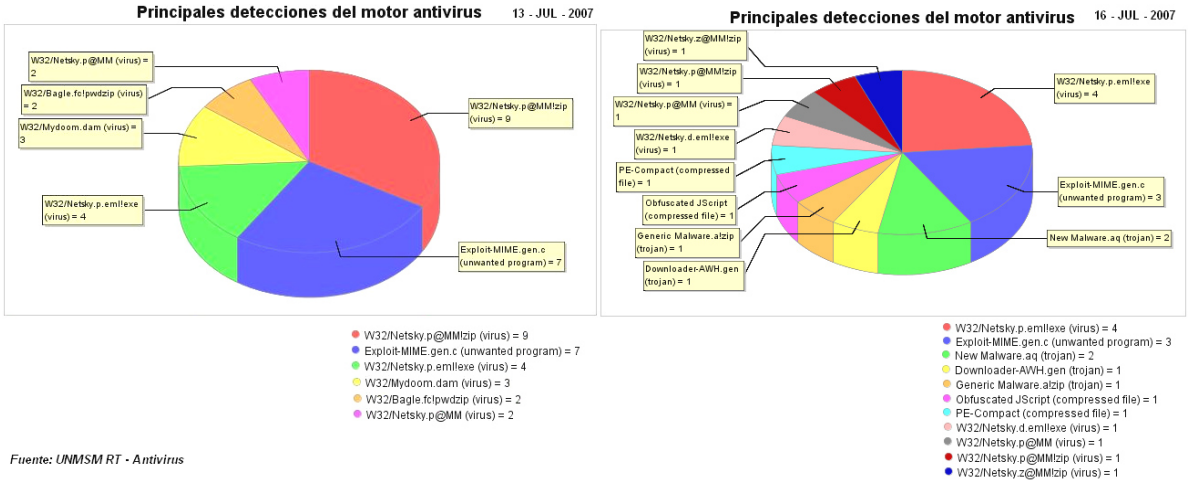



**Grafico Nº 10**

En este gráfico se aprecia la distribución entre el correo admitido y el correo no deseado.

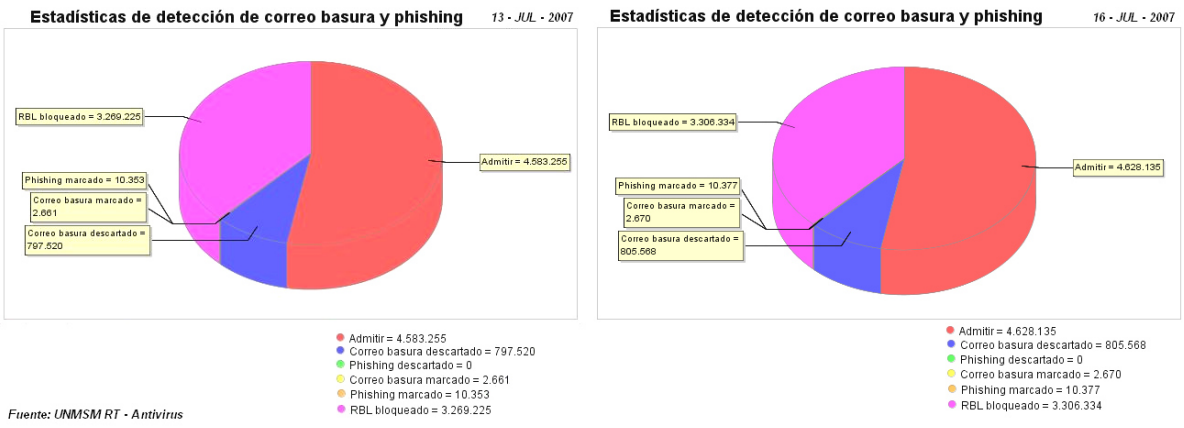



**Grafico Nº 11**

## La Seguridad Informática implementada en otras Universidades

Varias universidades en América Latina han implementado y vienen fortaleciendo su respectiva área de seguridad informática, esto debido a que hoy en día se presentan un mayor número de amenazas.

Como se puede apreciar, en el portal web de la Universidad Nacional de Colombia[1], en el espacio referido a la seguridad informática se puede encontrar la publicación de documentos sobre este tema, elaborados y propios de la entidad educativa. La elaboración de este tipo de normativas por parte de la entidad se debe al rápido avance tecnológico que trae consigo el aprendizaje y nuevas vulnerabilidades de lo cual el usuario no tiene conciencia, por ello se tiene la necesidad de especificar y definir un adecuado uso de las tecnologías de información, de tal modo que esto minimice el riesgo al que pueden verse expuestas de realizarse un uso inadecuado.

Pero hay instituciones que dan un paso más allá, como es el caso de la Universidad Autónoma de México, la cual cuenta con el Departamento de Seguridad en Cómputo/UNAM-CERT [2] que esta provisto de un laboratorio para la instrucción de futuros especialistas en este tema y que a la vez utilizan su conocimiento para el beneficio de la misma entidad. Y como uno de los puntos principales, toma en cuenta la concientización del usuario, lo que permitirá crear, fortalecer y extender una cultura informática a nivel de ellos.

---

[1] http://www.unal.edu.co/seguridad/index.html
[2] http://www.cert.org.mx/

## 1.2 Justificación e Importancia de la Investigación

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las instituciones en general para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos han llevado a que se desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la institución.

En este sentido, el Análisis de Riesgos en Seguridad Informática, como punto de inicio, dará origen a procedimientos y planes de seguridad, las cuales surgirán como una herramienta organizacional para concientizar a la comunidad universitaria sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la Universidad crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la institución, agudeza técnica para identificar riesgos y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

## 1.3 Delimitación del Problema

El ámbito físico geográfico es el Campus de la Universidad y las sedes externas que la componen. Esta investigación circunscribe su estudio a autoridades universitarias, personal docente, administrativo y estudiantes de la Universidad. Va a estar delimitado por el estándar internacional de seguridad informática ISO 17799.

# CAPÍTULO II

# 2. FORMULACION DEL PROBLEMA

## 2.1 Objetivos

### 2.1.1 Objetivos Generales

El objetivo del presente trabajo es realizar el Análisis de Riesgos en Seguridad Informática de la Universidad que permita dar inicio al desarrollo de procesos y procedimientos seguros basados en políticas y estándares recomendados por el estado peruano (ONGEI - Oficina Nacional de Gobierno Electrónico e Informática) y el ISO 17799, completo conjunto de controles, internacionalmente reconocidos, que abarcan las mejores prácticas en materia de seguridad de la información.

Adicionalmente, el presente trabajo contempla:

- Dar los alcances de solución para cada factor de riesgo identificado.
- Promover una cultura de seguridad informática entre toda la comunidad universitaria: autoridades, administrativos, docentes y alumnos; como un medio para proteger los sistemas de información.

### 2.1.2 Objetivos Específicos

- Estudiar los riesgos que soporta un sistema de información, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.
- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

## 2.2 Definición del Problema

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de Internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crakers, etc., es decir transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un contínuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país no existe una sola institución que no se haya visto sujeta a los ataques en sus instalaciones, tanto desde el interior como del exterior, basta decir que cuando en el centro estamos sujetos a un ataque un grupo

de gente se involucran y están pendientes de éste, tratando de contrarrestar y anular estas amenazas reales.

Nuestra carencia de recursos humanos involucrados en seguridad, la escasa concientización, la falta de visión y las limitantes económicas han retrasado el plan rector de seguridad que se requiere.

Es deber del administrador de red realizar la búsqueda de las vulnerabilidades existentes en la red de datos, pero la mayoría de las veces no se sabe por donde empezar, que investigar o que preguntar. Además el problema mayor que tienen estos es que no atacan el problema de fondo, sino que aplican parches superficiales, como instalando programas en los equipos y así disminuyendo el rendimiento de las maquinas.

En la actualidad un administrador de red no se preocupa mucho de la seguridad, pero cuando llega a tener problemas el tiempo que emplea es mucho mayor al que podría demorar si existiera alguna política o procedimiento para el uso correcto de los recursos informáticos. Sin la búsqueda de vulnerabilidades, las empresas crean una idea errada de su seguridad, piensan que la seguridad de su información es muy poco vulnerable, ya sea porque nunca se han visto afectados o tal vez lo están siendo sin saberlo.

El objetivo principal de la Dirección de Telemática es brindar a los usuarios los recursos informáticos con la cantidad y calidad que demandan, esto es,

que se tenga un servicio continuo y confiable los 365 días del año. Así, la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta la Universidad son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

# CAPÍTULO III

# 3. MARCO TEORICO CONCEPTUAL

## 3.1 Antecedentes de la Investigación

### 3.1.1 ¿Qué es la Seguridad?

Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de *seguridad* y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de *seguridad*; por tanto, se habla de *sistemas fiables* en lugar de hacerlo de *sistemas seguros*.

A grandes rasgos se entiende que mantener un sistema *seguro* (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. ¿Qué implica cada uno de estos tres aspectos? La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en

disponible para otras entidades; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio (una modalidad de ataque). Generalmente tienen que existir los tres aspectos descritos para que haya seguridad.


**Gráfico N° 12 – Seguridad de la Información**

### ¿Qué queremos Proteger?

Los tres elementos principales a proteger en cualquier sistema informático son el *software*, el *hardware* y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, disquetes...) o tarjetas de red. Por software entendemos el conjunto de programas lógicos que hacen funcional al *hardware*, tanto sistemas operativos como aplicaciones, y por datos el conjunto de información lógica que manejan el *software* y el *hardware*, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar.

Contra cualquiera de los tres elementos descritos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos autores consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado.

**¿De qué nos queremos proteger?**

En la gran mayoría de publicaciones relativas a la seguridad informática en general, tarde o temprano se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. Con frecuencia,

especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad, se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. Pero es preferible hablar de elementos y no de personas: aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de personas, como por ejemplo programas, catástrofes naturales o por elementos desconocidos; si un usuario pierde un trabajo importante a causa de un ataque, poco le importará que haya sido un intruso, un gusano o un simple error del administrador.

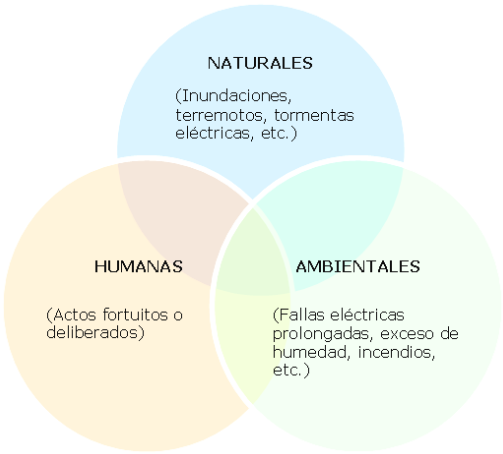



**Gráfico Nº 13 – Factores de Riesgo**

## ¿Cómo nos podemos proteger?

Hasta ahora se ha mencionado los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar la visión de la seguridad, se ha de mencionar las formas de protección de los sistemas.

Para proteger un sistema debemos realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis se deberá diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina mecanismos de seguridad; son la parte más visible del sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación. Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema en la red. Por mecanismos de detección se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría. Finalmente, los mecanismos de recuperación son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware

adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de la red.

Parece claro que, aunque los tres tipos de mecanismos son importantes para la seguridad del sistema, se debe enfatizar en el uso de mecanismos de prevención y de detección; la máxima popular “más vale prevenir que lamentar” se puede aplicar a la seguridad informática: evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar el estado tras una penetración de la máquina. Es más, un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante mecanismos de prevención de una forma completa, no necesitaría mecanismos de detección o recuperación. Aunque esto es imposible de conseguir en la práctica, será en los mecanismos de detección, y sobre todo en los de prevención, en los que se centra este trabajo.

Ejemplos de mecanismos de prevención más habituales en Unix y en redes son los siguientes:

- *Mecanismos de autenticación e identificación:* Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto. Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios.

- *Mecanismos de control de acceso:* Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.

- *Mecanismos de separación:* Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso. Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación.

- *Mecanismos de seguridad en las comunicaciones:* Es especialmente importante para la seguridad del sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, comúnmente se utilizan ciertos mecanismos, la mayoría de los cuales se basan en la Criptografía: cifrado de clave pública, de clave privada, firmas digitales. Aunque cada vez se utilizan más los protocolos seguros (como SSH o Kerberos, en el caso de sistemas Unix en red), aún es frecuente encontrar conexiones en texto claro ya no sólo entre máquinas de una misma subred, sino entre redes diferentes. Una de las mayores amenazas a la integridad de las redes es este tráfico sin cifrar, que hace extremadamente fáciles ataques encaminados a robar contraseñas o suplantar la identidad de máquinas de la red.

### 3.1.2 Evolución del Malware

**El Primer Virus: Elk Cloner**

Según el artículo de Wikipedia "Virus de Computadora"[3], el primer virus de computadora encontrado en estado natural, fuera de los laboratorios de investigación, fue "Elk Cloner" en 1982 escrito por Rich Skrenta, entonces un adolescente en California Meridional.

El virus fue aparentemente no destructivo, su propósito principal fue de molestar a los amigos de Skrenta para devolverle disquetes prestados.

[3] http://es.wikipedia.org/wiki/Virus_de_computadora

El código se ejecutó en una máquina Apple II y se conectaba al sistema de archivos de Apple DOS.

Apple DOS y sus sucesores de monousuario tal como MacOS hasta el System 9 vieron la actividad ocasional del virus los años siguientes, de igual modo que muchos de los otros sistemas personales de la era los cuales tenían limitadas o ninguna característica de seguridad incorporada en el sistema.

**El Primer Virus para Pc: (C)Brain**

Tomó unos pocos años para el mundo de la computadora personal el ser alcanzada. El código de virus más precoz para el PC en ser encontrado en estado natural fue una porción de software llamada (c)Brain, que fue escrito y extendido por todo el mundo en 1986. (c)Brain se adhería al sector inicio en los disquetes. En contraste con un número pequeño de variantes de malware para PC a seguir, este virus en particular no fue especialmente destructivo más allá del daño hecho alterando los sectores del inicio.

Como la mayor parte de los sistemas de computadora personal populares de la era, el MS-DOS no tenía características esenciales de seguridad en todo lo que representa. En retrospectiva era probablemente inevitable que el malware de computadora se convirtiera en un problema mayor.

Con vendedores de sistemas incapaces o no dispuestos a reescribir los sistemas operativos para eliminar los bugs que permitían que los gusanos se propaguen, una industria entera creció de la enumeración de vulnerabilidades. Hasta este día una gran parte del sector de computadoras basadas en TI continúa dedicado a escribir malware y a producir las más elaboradas soluciones para las fallas básicas del sistema MS-DOS y sus descendientes. Las listas actuales de virus típicamente contienen firmas para aproximadamente 100,000 variantes de malware de computadora personal principalmente.

**El Primer Gusano para Unix: El Gusano Morris**

Mientras tanto en el mundo Unix, con su base mas estable y relativamente sus usuarios bien entrenados, las cosas estuvieron relativamente tranquilas, por lo menos un rato. La paz fue más o menos quebrantada el 2 de noviembre de 1988 cuando el primer gusano para Unix, el gusano Morris golpeó las máquinas Unix en los inicios de Internet. Este fue el primer gusano que se replicó en un ambiente Unix y el primer ejemplo de un gusano que utilizó la red para propagarse.

Casi 20 años más tarde, aun hay una cantidad asombrosa de información de este gusano disponible en la red, incluyendo lo que parece ser el código fuente completo del gusano mismo y un número de análisis por personas sumamente competentes. Parte de las características del gusano Morris le será familiar.

• Fue elaborado para un sistema específico - aunque hay indicios de que el gusano fue pensado para ejecutarse en más arquitecturas, en realidad solo fue capaz de ejecutarse exitosamente en máquinas VAXes y sun3 que ejecutan BSD.

• Explotó bugs y vulnerabilidades - como muchos de todos sus sucesores, el gusano Morris explotaba bugs en programas comunes, tal como un vaciado de búfer en el fingerd (programa de escaneo de puertos de Unix), utilizaba el modo debug comúnmente habilitado en el sendmail – el que permitió la ejecución remota de comandos - junto con un diccionario corto de contraseñas probables.

• Se replicaba y difundía - una vez que el gusano entraba, empezaba el proceso de difusión. Afortunadamente, el gusano fue diseñado principalmente para expandirse, no para hacer algún daño.

• Lleva al estado de negación del servicio – Desgraciadamente, el mismo código del gusano tenía un bug que hizo más eficiente la distribución de lo que su autor había anticipado, y causó un aumento grande en el tráfico de la red, haciendo más lento el tráfico de Internet a muchos hosts. Algunos hosts solucionaron el problema desconectándose de Internet temporalmente. En cierto modo, puede haber sido uno de los primeros incidentes registrados de "Negación de Servicio".

Se estimó que el gusano pudo haber alcanzado aproximadamente el 10% de los hosts conectados a Internet en aquel momento, y la mejor estimación comúnmente citada de un número absoluto es "alrededor de 6.000 hosts".

El acontecimiento fue bastante estresante para, según los estándares de hoy en día, un grupo muy pequeño de personas. En retrospectiva, es probablemente justo decir que el episodio sirvió principalmente para hacer caer en cuenta a los usuarios en general que había un potencial para los problemas de seguridad, y los desarrolladores y administradores del sistema emprendieron el arreglo de estos.

**Microsoft e Internet**

Los componentes finales para formar el desorden actual llegaron a escena en la segunda parte de los años noventa cuando Microsoft introdujo componentes modernos de networking al setup predefinido en su sistema de software para computadora personal que venía preinstalado en las computadoras. Esto sucedía aproximadamente al mismo tiempo que varias aplicaciones de oficina se empezaron a embarcar en un entorno de programación de lenguaje macro.

Encaminándose hacia la temprana comercialización de los años noventa de Internet, Microsoft empezó a realizar verdaderos esfuerzos para elaborar una interfaz de comunicación con Internet a mediados de los años noventa. Hasta hacia algún tiempo en 1995, la conexión a Internet

era un extra opcional para los usuarios de Microsoft, principalmente a través de programas de terceros y con frecuencia por medio de difíciles configuraciones para conexiones dial-up.

Así como los programas de terceros, la propia pila TCP/IP de Microsoft era un extra opcional – descargable sin costo, pero no instalado por defecto hasta las ediciones últimas de Windows 3.11 que empezaron a entregarse con la pila TCP/IP por defecto.

El original servicio de Red de Microsoft tuvo algunas limitaciones de conexión a Internet; evidencias anecdóticas indican que una sencilla transmisión de correo electrónico a usuarios de Internet y la respuesta podría tomar varios días de cada manera en cada sentido.

Para suerte o desgracia, en el tiempo de la aventura de Internet que Microsoft empezó, varias de sus aplicaciones habían sido extendidas para incluir lenguajes de programación macro los cuales eran entornos de programación completos.

En retrospectiva podemos indicar seguramente que los escritores de malware se adaptaron más rápidamente a las circunstancias cambiantes que Microsoft. La combinación de conectividad de red, poderosos lenguajes y aplicaciones macro que ingresaron a la red en un nivel pero no tenían incorporado realmente ningún concepto importante de

seguridad y, por supuesto, el gran número de objetivos disponibles demostraron que eran imposibles de resistir.

Al final de la década del noventa e inicios del 2000 se vió una corriente constante de malware a través de Internet en la plataforma de Microsoft, algunas veces con varias nuevas variantes cada día. Un muestreo aleatorio de los más espectaculares incluye Melissa, ILOVEYOU, Sobig, Code Red, Slammer y otros; algunos fueron bastante destructivos, mientras que otros fueron simplemente muy eficientes en esparcir su carga útil.

Todos ellos explotaban bugs y malas configuraciones comunes tal como el gusano Morris lo había hecho con anterioridad una década o más. Las notas de junio del 2000 de Greg Lehey[4] sobre uno de los gusanos más peligrosos aun valen la pena leer. La descripción es una de muchas indicaciones que por el año 2000, los escritores de malware habían aprendido a extraer datos de los buzones de correo de sus víctimas y de sus listas de contacto para obtener datos útiles.

Durante esos mismos años, la postura de Microsoft se desarrolló en cierto modo. Su respuesta tradicional había sido "*Nosotros no tenemos bugs"*, luego se movieron gradualmente a liberar parches y "hot fixes" a una tasa creciente, y finalmente se movieron al régimen mensual "Parche del martes" a modo de introducir alguna previsibilidad a sus clientes.

[4] http://ezine.daemonnews.org/200006/dadvocate.html

**Características del Malware Moderno**

En el pasado, el software malicioso y destructivo tenía toda la atención. De vez en cuando un virus, gusano u otro malware podía llenarse de titulares por la destrucción de sistemas de personas, en algunos casos por sobreescribir los sistemas BIOS's de una variedad común de PC. No se tiene cifras cuantificadas reales, pero una teoría probable es que durante aquellos primeros años los escritores de malware podrían haber sido principalmente bromistas juveniles y académicos extraños, y la obtención de atención pudo haber sido el motivo principal.

En contraste, el malware moderno trata de tomar su sistema sin hacer daño alguno al usuario o menos notorio que el administrador del sistema no lo pueda advertir. El típico malware en estos días envía su carga útil la cual luego procede a tomar el control de la computadora – convirtiéndola en un zombi, generalmente para mandar spam, para infectar otras computadoras, o para realizar cualquier función que necesite el cliente del escritor del malware para ser hechas por mando a distancia.

Hay amplia evidencia de que una vez que las máquinas son tomadas, el malware instalado podría probablemente registrar las pulsaciones de teclas de los usuarios, buscar información financiera o de identificación en los archivos del sistema, y por supuesto cualquier otro tipo de actividad de red controlada remotamente tal como la participación en ataques en redes específicas. Hay también evidencia anecdótica para sugerir que un subconjunto significativo de jugadores de casino en línea

son en realidad jugadores robot controlados ejecutándose en computadoras comprometidas.

El Programa CERT[5] forma parte del Instituto de Ingeniería de Software (SEI - Software Engineering Institute), un centro de investigación y desarrollo tecnológico financiado federalmente en la Universidad de Carnegie Mellon en Pittsburgh, Pennsylvania. Seguido al incidente del gusano Morris, que detuvo el 10 por ciento de sistemas de Internet en noviembre 1988, la Agencia de Proyectos de Investigación de Defensa Avanzada (DARPA) encargó al SEI establecer un centro para coordinar la comunicación entre expertos durante emergencias de seguridad y para ayudar a prevenir incidentes en el futuro. Este centro fue denominado el Centro de Coordinación CERT (CERT/CC).

Mientras continuaron respondiendo a la mayoría de incidentes de seguridad y analizando vulnerabilidades de productos, su papel se ha ampliado con el paso de los años. Junto con el rápido aumento en el tamaño de Internet y su uso para funciones críticas, ha habido cambios progresivos en las técnicas de intrusión, aumento en la cantidad de daños, aumento en la dificultad de detectar un ataque, y aumento en la dificultad de atrapar a los atacantes. Para manejar mejor estos cambios, el CERT/CC es ahora parte del más grande Programa CERT, el cual desarrolla y promueve el uso de tecnología apropiada y prácticas de administración de sistemas para resistir los ataques en sistemas de red,

[5] http://www.cert.org/

para limitar el daño, y para asegurar la continuidad de los servicios críticos.

## 3.2 Bases Teóricas

### 3.2.1 Misión y Objetivos de la Universidad

#### Misión

La Universidad Nacional Mayor de San Marcos[6], fundada en 1551, es una comunidad académica dedicada a la formación de profesionales de alto nivel, cultos, generadores de conocimientos, críticos, comprometidos con la búsqueda de la verdad y la práctica de valores; a la investigación científica, tecnológica y humanística, y a la integración social que contribuya con el desarrollo sostenible de la sociedad y el medio ambiente.

#### Objetivos Estratégicos Generales

#### Formación

1. Formar profesionales integrales: competitivos, cultos, con espíritu crítico y creativo, líderes en su especialidad, generadores de conocimientos, con valores y comprometidos con el desarrollo de la sociedad.

[6] http://www.unmsm.edu.pe

**Docencia**

2. Contar con una plana docente de alto nivel académico pedagógico, con compromiso ético, moral y social, que contribuya a la formación de profesionales integrales.

**Producción de conocimientos**

3. Establecer la generación de conocimientos, con énfasis en la investigación científica, tecnológica y humanística, como eje fundamental del desarrollo de la universidad, orientado a resolver los problemas prioritarios de la sociedad.

**Integración Social**

4. Hacer de la integración social un pilar para el desarrollo de la universidad, estableciendo canales de interacción entre universidad, Estado, empresa e instituciones sociales, hacia un desarrollo integral y sostenible.

**Gestión**

5. Desarrollar una cultura organizacional de excelencia basada en principios y valores que permita una gestión de alta calidad.

### 3.2.2 El Estado Peruano y la Seguridad Informática

El estado peruano tiene como organismos encargados de las tecnologías de información y seguridad informática al Instituto Nacional de Estadística e Informática (INEI) y la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).

**INEI**

El Instituto Nacional de Estadística e Informática (INEI)[7] es el órgano rector de los Sistemas Nacionales de Estadística e Informática en el Perú. Norma, planea, dirige, coordina, evalúa y supervisa las actividades estadísticas e informáticas oficiales del país.

Para el cumplimiento de sus objetivos y funciones cuenta con autonomía técnica y de gestión, establecido en su Ley de creación.

**Misión**

Contribuir a la toma de decisiones con información estadística de calidad y al uso de tecnologías de información para el desarrollo de la sociedad.

**Funciones**

Entre las principales funciones del INEI tenemos:

- Formular y evaluar la Política y el Plan Nacional de Estadística e Informática; así como, coordinar y orientar la formulación y evaluación de los planes sectoriales, regionales, locales e institucionales.
- Normar, supervisar y evaluar los métodos, procedimientos y técnicas estadísticas e informáticas utilizados por los órganos del Sistema.
- Establecer normas y estándares nacionales para la regulación y compatibilización de los sistemas de tratamiento de la información.

[7] http://www.inei.gob.pe

- Coordinar sobre normas y estándares para la implementación de sistemas de comunicación entre computadoras, en el ámbito regional y nacional.
- Promover el desarrollo de sistemas y aplicaciones informáticas de uso común para el sector estatal, en las regiones y a nivel nacional.
- Coordinar la transferencia de Sistemas Informáticos desarrollados a aquellos organismos del estado que no lo disponen, y, ejecutar actividades que por economía de escala solo se justifican efectuarlas centralmente para las entidades del estado, a nivel regional.
- Desarrollar y administrar el Banco Nacional de Información, así como normar el desarrollo y administración de los Bancos de Datos de los órganos integrantes de los Sistemas.
- Celebrar convenios sobre asistencia técnica, capacitación especializada y prestación de servicios de carácter estadístico e informático.
- Normar, orientar y evaluar la organización de las Oficinas de Estadística e Informática del Sistema; así como promover la creación de Oficinas de Estadística y/o Informática.
- Coordinar con los organismos responsables de la normatividad respecto a los planes contables, a fin de facilitar la captación de la información estadística y el procesamiento electrónico de datos.
- Coordinar, opinar y apoyar en los proyectos de prestación de asistencia técnica financiera nacional e internacional, que en materia de estadística o informática, requieran los órganos del Sistema Estadístico y/o Informático Nacional en todos sus niveles.

- Cautelar la confidencialidad de la información, producida por los órganos de los sistemas.
- Reconocer y garantizar el derecho de la propiedad intelectual de los autores de programas de computación.
- Oficializar reportes y medios magnéticos emitidos por los órganos de los Sistemas.
- Producir y consolidar información e instrumentos informáticos para los fines de la seguridad nacional.

**ONGEI**

La PCM (Presidencia del Consejo de Ministros) a través de la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática) [8], se encarga de normar, coordinar, integrar y promover el desarrollo de la actividad informática en la Administración Pública (DS Nº 066-2003-PCM, DS Nº 067-2003-PCM).

**Funciones**

La ONGEI tiene las siguientes funciones:

- Proponer la Estrategia Nacional de Gobierno Electrónico, así como coordinar y supervisar su implementación.
- Proponer las iniciativas para el mejoramiento de procesos administrativos y técnicos en el proceso de implementación del Gobierno Electrónico.
- Desarrollar acciones orientadas a la consolidación y desarrollo del Sistema Nacional de Informática, proponer las directivas para su

[8] http:// www.**ongei**.gob.pe

funcionamiento y supervisar el cumplimiento de la normativa correspondiente.

- Coordinar y supervisar la integración funcional de los sistemas informáticos del Estado y promover el desarrollo de sistemas y aplicaciones de uso común en las entidades de la Administración Pública.
- Coordinar y supervisar el desarrollo de los portales de las entidades de la Administración Pública para facilitar la interrelación de las entidades entre sí y de éstas con el ciudadano, con el fin de establecer la ventanilla única de atención.
- Administrar el Portal del Estado Peruano.
- Proponer los lineamientos de la política de contrataciones electrónicas del Sistema Electrónico de Contrataciones y Adquisiciones del Estado – SEACE.
- Brindar asistencia técnica a las entidades de la Administración Pública para la implementación de proyectos tecnológicos en materia de su competencia.
- Formular propuestas para impulsar el proceso de desarrollo e innovación tecnológica para la mejora de la gestión pública y modernización del Estado promoviendo la integración tecnológica.
- Aprobar los estándares tecnológicos para asegurar las medidas de seguridad de la información en las entidades de la Administración Pública.
- Fomentar una instancia de encuentro con representantes de la Administración Pública y del Sector Privado, con el fin de coordinar y

potenciar los distintos esfuerzos tendientes a optimizar un mejor aprovechamiento de las nuevas tecnologías aplicadas a la modernización de la gestión pública.

**Publicaciones de la ONGEI**

***Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana – 2005:*** En este documento, se presentan las políticas, estrategias, acciones y metas que deberán ser impulsadas por todos los sectores del país, tiene el claro norte de generar una Sociedad de la Información en el Perú, que permita obtener eficiencias, habilitando la disponibilidad de cualquier tipo de información, servicios o contenidos electrónicos a sus integrantes. El libro presenta un diagnóstico de la realidad peruana y su contexto mundial, respecto a la Sociedad de la Información, para dar paso a los factores críticos de éxito del plan, establecer la visión y desarrollar cinco objetivos estratégicos, relacionados a los temas de Infraestructura de Telecomunicaciones, Desarrollo de Capacidades Humanas, Aplicaciones sociales, participación ciudadana y desarrollo, Producción y servicios y finalmente Gobierno Electrónico. Su publicación fue aprobado por Resolución Ministerial N° 148 - 2005 - PCM.

***Política Nacional de Informática:*** Documento donde se establece los principios y acciones para modernizar la gestión pública y propiciar la descentralización del Estado mediante el uso intensivo de las tecnologías de información, promover el incremento de capacidades

competitivas en la Administración Pública, empresas y ciudadanos por medio del uso intensivo de las TI, entre otros.

***Plan de Desarrollo Informático 2003 – 2006:*** Es un instrumento de gestión directriz e integrador de las propuestas y proyectos orientados a mejorar la eficiencia y eficacia de las instituciones para lograr un estado democrático, descentralizado y al servicio del ciudadano en las perspectivas que las actividades informáticas que se desarrollan permitan el fortalecimiento del Sistema Nacional de Informática

***Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI:*** Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la gestión de la Seguridad de la Información.

### 3.2.3 Estándares de Seguridad Informática

Los estándares BS 7799/ISO 17799 pueden ser utilizados como una base para desarrollar estándares de seguridad y prácticas de administración de la seguridad dentro de las organizaciones. El código de prácticas del DTI (en el Reino Unido, Departamento de Comercio e Industria) para la seguridad de información que fue desarrollada con el apoyo de la industria en 1993 se convirtió en el Estándar Inglés (BS – British Standard) 7799 en 1995. Este estándar fue subsiguientemente revisado en 1999 para agregarle los componentes de certificación y acreditación, que se convirtieron en la parte 2 del estándar. La parte 1

del estándar BS 7799 se convirtió en el ISO 17799 y fue publicado como ISO 17799:2000 como el primer estándar internacional de administración de la seguridad de la información por la Organización Internacional de Estándares (ISO) y la Comisión Electrotécnica Internacional (IEC).

El estándar ISO 17799 fue modificado en junio del 2005 como ISO/IEC 17799:2005 y contiene 134 controles detallados de seguridad de información basados en las siguientes 11 áreas:

- Política de seguridad de la información
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Conformidad

Los estándares ISO están agrupados por áreas de tema, y la serie ISO/IEC 27000 ha sido designada como la serie de la administración de seguridad de la información. Por ejemplo, el 27002 Guía de Buenas Practicas reemplazará el actual ISO/IEC 17799:2005 Tecnología de la Información - Técnicas de Seguridad - Código de Practicas para la

Administración de la Seguridad de los Sistemas de Información. Esto es consecuente con cómo ISO ha denominado otras áreas del tema, tal como la serie ISO 9000 para la administración de la calidad.

ISO/IEC 27001:2005 fue publicado en octubre del 2005, y especifica los requisitos para establecer, implementar, operar, controlar, revisar, mantener y mejorar un sistema documentado de la administración de la seguridad de información según el famoso “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), tomando en consideración los riesgos del negocio de la compañía. Este estándar de administración fue basado en el BS 7799, parte 2 del estándar y proporciona información en la construcción de sistemas de administración de seguridad de la información así como pautas para auditar esos sistemas.

El uso apropiado de los estándares es crítico dentro de una organización. Los estándares ayudan a definir y detallar los requisitos para la administración de la seguridad dentro de una organización. Como ha determinado la Organización Internacional de Estándares en el estándar BS ISO/IEC 27001:2005, la administración de la seguridad, en la forma de la implementación y certificación de un sistema de administración de la seguridad de información, proporciona consideraciones para las personas, procesos, datos, tecnología, y facilidades. Este estándar prescribe una estructura cohesiva y mutuamente dependiente que permite la implementación apropiada de

los principios de administración de la seguridad dentro de una organización.

Como se indica en el sitio web Standards Direct[9], "la ISO 27001 es una "especificación" para un ISMS (Information Security Management System - Sistema de Administración de Seguridad de Información), oficialmente titulada Tecnología de la Información - Técnicas de Seguridad - Sistema de Administración de la Seguridad de la Información - Requerimientos". La ISO 27001 reemplaza a la BS 7799-2:2002 que describió la especificación previa para ISMS. Este estándar esta de acuerdo con el ISO 17799 que es considerado como una Guía de practicas para la seguridad de información y la BS 7799, del cual la última versión, BS 7799-3:2006, es titulado Sistemas de Administración de Seguridad de Información - Pautas para la Gestión de Riesgos de la Seguridad de Información.


**Gráfico Nº 14 – Modelo PDCA (Plan-Do-Act-Check)**

[9] http://17799.standardsdirect.org/

### 3.2.4 Administración de Riesgos - Marco Conceptual de Administración de Riesgos

**¿Qué es Administración de Riesgos?**

La administración de riesgos es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales.

Es entonces la administración de riesgos el término asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos de la Organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades.

**Beneficios de la Administración de Riesgos**

Organizaciones que han aplicado enfoques efectivos de administración de riesgos han reportado entre otros los siguientes beneficios:

A nivel organizacional:

- Alcance o logro de los objetivos organizacionales.
- Énfasis en prioridades de negocio: permite a los directivos enfocar sus recursos en los objetivos primarios. Tomar acción para prevenir y reducir pérdidas, antes que corregir después de los hechos, es una estrategia efectiva de administración del riesgo.
- Fortalecimiento del proceso de planeación.

- Apoyo en la identificación de oportunidades.
- Fortalecimiento de la cultura de autocontrol.

Al proceso de administración:

- Cambio cultural que soporta discusiones abiertas sobre riesgos e información potencialmente peligrosa. La nueva cultura tolera equivocaciones pero no tolera errores escondidos. La nueva cultura también hace énfasis en el aprendizaje de los errores.
- Mejor administración financiera y operacional al asegurar que los riesgos sean adecuadamente considerados en el proceso de toma de decisiones. Una mejor administración operacional generará servicios más efectivos y eficientes. Anticipando los problemas, los directivos tendrán mayor oportunidad de reacción y tomar acciones. La organización será capaz de cumplir con sus promesas de servicio.
- Mayor responsabilidad de los administradores en el corto plazo. A largo plazo, se mejorarán todas las capacidades de los directivos.

**Características Generales**

- La Administración de Riesgos debe estar apoyada por la Alta Gerencia de la Organización.
- La Administración de Riesgos debe ser parte integral del proceso administrativo utilizado por la Dirección de la Organización.
- La Administración de Riesgos es un proceso multifacético y participativo, el cual es frecuentemente mejor llevado a cabo por un equipo multidisciplinario.

**Etapas del Proceso de Administración de Riesgos**

A continuación se describen las principales etapas definidas para el Proceso de Administración de Riesgos.

**1. Establecimiento del Contexto General**

Permite, a través del conocimiento del entorno y de la organización, establecer las políticas y criterios generales que serán utilizados para implementar el enfoque de Administración de Riesgos en cualquier área de la Organización.

Durante esta etapa se deben establecer las políticas y criterios generales que serán utilizados para la aplicación del enfoque de Administración de Riesgos en cualquier área de la organización.

Consiste en identificar las relaciones entre la organización y su entorno, entender la organización, sus objetivos, estrategias, capacidades y habilidades, así como identificar todos aquellos objetos (áreas, procesos, proyectos, etc.) de la organización a los cuales se podría aplicar un Análisis de Riesgos, y permite determinar, mediante el uso de los criterios generales, definidos previamente, sobre cuales de ellos debe realizarse el análisis

**2. Identificación de Riesgos**

Mediante el establecimiento de un marco de acción específico que permita entender el objeto sobre el cual se aplicará el proceso de Administración de Riesgos. Consiste además, en definir los criterios

específicos del análisis de riesgos y determinar el nivel de aceptación de riesgo que la organización está dispuesta a aceptar para este proceso. El propósito final de esta etapa es proveer los mecanismos necesarios para recopilar la información relacionada con los riesgos, impactos y sus causas.

Importante en esta etapa, es la definición de Riesgo. Para la mayoría de partes, los riesgos son percibidos como cualquier cosa o evento que podría apoyar la forma en que la organización alcance sus objetivos.

Por consiguiente, para estas organizaciones, la administración de riesgos no se realiza sobre “riesgos adversos”. La administración de riesgos no está dirigida exclusivamente a evitarlos. Su enfoque está en identificar, evaluar, controlar y “dominar” los riesgos. Administración de riesgos también significa tomar ventaja de las oportunidades y tomar riesgos basados en decisiones informadas y análisis de resultados.

**3. Análisis del Riesgos**

En esta etapa se busca obtener el entendimiento y conocimiento de los riesgos identificados de tal manera que se pueda recopilar información que permita el cálculo del nivel de riesgo al cual está expuesto el objeto en la actualidad, Identificar los controles existentes implementados para mitigar el impacto ante la ocurrencia de los riesgos, permitiendo de esta manera valorar los niveles del riesgo, la efectividad de los controles y el nivel de exposición.

El riesgo es analizado a través de la combinación de estimativos de probabilidad y de las consecuencias en el contexto de las medidas de control existentes. El análisis de riesgos involucra un debido examen de las fuentes de riesgo, sus consecuencias y la probabilidad de que esas consecuencias puedan ocurrir. Pueden llegar a identificarse factores que afectan tanto las consecuencias como la probabilidad.

Los estimativos pueden determinarse utilizando análisis, estadísticas y cálculos. Alternativamente donde no hay datos históricos disponibles, se pueden hacer estimativos subjetivos que reflejen el grado de creencia de un grupo o de un individuo en que un evento en particular o suceso ocurran.

**4. Evaluación y Priorización de Riesgos**

La evaluación de riesgos incluye comparar el nivel de riesgo encontrado durante el proceso de análisis contra el criterio de riesgo establecido previamente, y decidir si los riesgos pueden ser aceptados.

El análisis de riesgos y los criterios contra los cuales los riesgos son comparados en la valoración deben ser considerados sobre la misma base. Así, evaluaciones cualitativas incluyen la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y evaluaciones cuantitativas involucran la comparación de niveles estimados de riesgo contra criterios que pueden ser expresados como números específicos, tales como fatalidad, frecuencia o valores monetarios.

El resultado de una evaluación de riesgos es una lista priorizada de riesgos para definirles acciones de tratamiento posteriores.

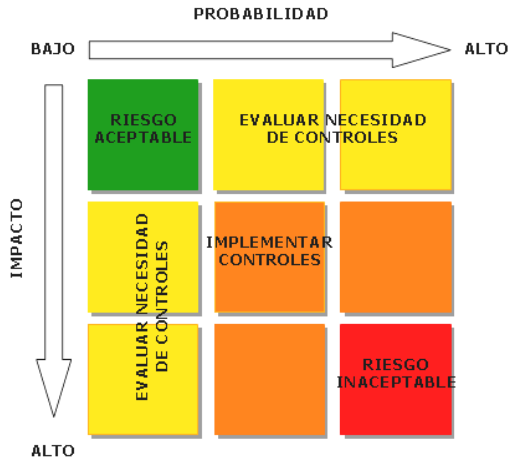



**Grafico Nº 15 – Evaluación del Impacto para el Negocio**

## 5. Tratamiento de Riesgos

Después de valorar y priorizar los riesgos, y dependiendo del nivel de exposición, se debe determinar la opción de tratamiento que más conviene aplicar en cada caso. El tratamiento de riesgos incluye la identificación de la gama de opciones de tratamiento del riesgo, la evaluación de las mismas, la preparación de planes de tratamiento de riesgos y su posterior implementación.

Las opciones de tratamiento que se relacionan a continuación no son mutuamente exclusivas ni serán apropiadas en todas las circunstancias:

- EVITAR el riesgo: Se decide, donde sea práctico, no proceder con servicios, procesos y/o actividades que podrían generar riesgos inaceptables, buscando con ello eludir el riesgo inherente asociado a

esos objetos. Es siempre la primera alternativa que debe considerarse.

- REDUCIR el riesgo: La organización decide prevenir y/o reducir el riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible, el cual debe ser compatible con las actividades de las áreas. Se consigue mediante la optimización de los procedimientos y la implementación de controles.
- *REDUCIR la probabilidad de ocurrencia:* Prevención del riesgo a través de la implementación de acciones tendientes a controlar su frecuencia o probabilidad.
- *REDUCIR las consecuencias o MITIGAR el riesgo:* reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste ocurre.
- ATOMIZAR el riesgo: La organización decide segmentar el objeto sobre el cual recae la amenaza de riesgo o, distribuir la localización de los objetos.
- TRANSFERIR el riesgo. La organización decide traspasar o trasladar riesgos a otra parte o lugar de manera total o parcial. Las transferencias parciales son conocidas como COMPARTIR el Riesgo. La distribución o localización del riesgo en diversos lugares se conoce como DISPERSIÓN o ATOMIZACIÓN del riesgo.
- ASUMIR el riesgo: La organización decide aceptar los riesgos como ellos existen en la actualidad, y establece políticas o estrategias

financieras apropiadas para su tratamiento. En este caso la organización considera que el riesgo residual actual es de nivel bajo y decide convivir con él, aceptando la pérdida probable, con lo cual las estrategias de prevención se vuelven esenciales.

### 6. Monitoreo y Revisión

Pocos riesgos permanecen estáticos. Por lo tanto, riesgos y la efectividad de sus medidas de control necesitan ser monitoreados continuamente para asegurar que circunstancias cambiantes no alteren las prioridades.

Revisiones progresivas son esenciales para asegurar que los planes de la administración permanecen relevantes. Los factores que afectan la probabilidad y la consecuencia de un resultado pueden cambiar, al igual que los factores que afectan la viabilidad o el costo de las opciones de tratamiento.

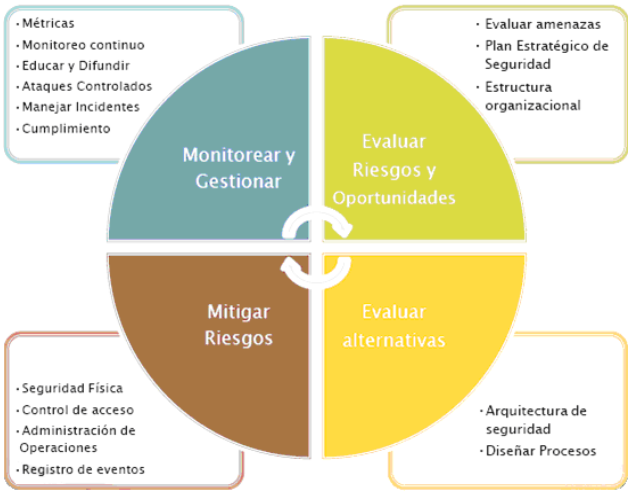



**Gráfico Nº 16 – La Administración del Riesgo es un proceso continuo**

## 3.3 Definición de Términos Básicos

***Adware:*** El término proviene de la síntesis de “Advertisement” y “Software”. El Adware, tal y como el mismo nombre sugiere, está concebido con el único propósito de promocionar o publicitar servicios y productos.

Este tipo de software comenzó por un lado a incluirse en programas tipo freeware o shareware (como moneda de cambio para su utilización gratuita), y por otro lado, empezó a vincularse a toda clase de websites que invitaban, engañaban o incluso forzaban a los navegantes para conseguir su instalación.

***Apple (Mac):*** Macintosh (abreviado Mac) es el nombre con el que actualmente nos referimos a cualquier computadora personal diseñada, desarrollada, construida y comercializada por Apple Inc.

***BIOS:*** El sistema básico de entrada/salida Basic Input-Output System (BIOS) es un código de interfaz que localiza y carga el sistema operativo en la RAM; es un software muy básico instalado en la placa base que permite que ésta cumpla su cometido. Proporciona la comunicación de bajo nivel, y el funcionamiento y configuración del hardware del sistema que, como mínimo, maneja el teclado y proporciona salida básica (emitiendo pitidos normalizados por el altavoz del ordenador si se producen fallos) durante el arranque.

***Bombas lógicas y bombas de tiempo:*** Son programas que no poseen rutinas de replicación y no pueden crear accesos remotos, pero son o

forman parte de aplicaciones que causarán daño o modificaciones a los datos si son activados. Pueden ser entes individuales o formar parte de gusanos o virus. Las bombas de tiempo están programadas para liberar su carga destructiva en un momento determinado. Las bombas lógicas están programadas para liberar su carga destructiva cuando ocurren determinados eventos. El principio de una bomba de tiempo también se puede aplicar en programaciones no maliciosas.

***BSD:*** Iniciales de Berkeley Software Distribution (en español, Distribución de Software Berkeley) y se utiliza para identificar un sistema operativo derivado del sistema Unix nacido a partir de las aportaciones realizadas a ese sistema por la Universidad de California en Berkeley.

***CERT:*** Es una organización destinada a asegurar que apropiadas prácticas de administración de tecnología y de sistemas sean utilizadas para resistir ataques en sistemas de red y para restringir el daño y asegurar la continuidad de servicios críticos a pesar de ataques exitosos, accidentes, o fallas. CERT no es una sigla. Es un nombre y una marca registrada del servicio.

***Cookie:*** Una información que la computadora acepta al conectarse a muchos sitios del internet. Es utilizado a través de su sesión como un medio para identificarle. La mayoría de los cookies son bastante inocuos, aunque algunos son maliciosos.

***Crakers:*** Usan su conocimiento con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal o moralmente inaceptable, piratería, fabricación de virus, herramientas de crackeo y elementos de posible terrorismo como la distribución de manuales para fabricar elementos explosivos caseros o la clásica tortura china.

***Crimeware:*** Criminalización del malware, es un tipo de software o programa informático que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos on-line mediante técnicas de Ingeniería Social u otras técnicas genéricas de fraude on-line, con el fin de conseguir el robo de identidades para acceder a los datos de usuario de las cuentas on-line de compañías de servicios financieros (típicamente bancos) o compañías de venta por Internet, con el objetivo de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.

***Criptografía:*** Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

***Debug:*** El debugging es un proceso metódico para encontrar y reducir el número de bugs, o de defectos, en un programa o una pieza de hardware electrónico haciendo que se comporte como se esperaba. La depuración

tiende a ser más difícil cuando varios subsistemas están trabajando simultáneamente, ya que los cambios en uno pueden causar bugs que surjan en el otro.

***Dial-up (Conexión por Línea Conmutada):*** Es una forma barata de acceso a Internet en la que el cliente utiliza un módem para llamar a través de la Red Telefónica Conmutada (RTC) al nodo del ISP (Proveedor de Servicios Internet), un servidor de acceso y el protocolo TCP/IP para establecer un enlace módem-a-módem, que permite entonces que se enrute a Internet.

***Exploit:*** Nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (llamadas bugs).

***Firewall:*** Elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red

***Fuzzy-fingerprint:*** Nueva técnica para atacar protocolos de autenticación de claves criptográficas que dependen de verificación humana de huellas claves. Es importante notar que fuzzy-fingerprint es un ataque contra un protocolo, no es un ataque criptográfico y tampoco ataca a ningún algoritmo criptográfico.

***Gusanos:*** Es un programa que una vez ejecutado se replica sin necesidad de la intervención humana. Se propagará de anfitrión en anfitrión haciendo uso indebido de un servicio(s) desprotegido(s). Atravesará la red sin la necesidad de que un usuario envíe un archivo o correo infectado.

***Hackers:*** Aficionados a la informática que buscan defectos, puertas traseras y mejorar la seguridad del software, así como prevenir posibles errores en el futuro.

***Hotfix:*** Es un paquete que puede incluir varios archivos y que sirve para resolver un bug específico dentro de una aplicación informática.

***Kerberos:*** Protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura.

***Lammers:*** Una persona que alardea de pirata informático, cracker o hacker y solo intenta utilizar programas de fácil manejo realizados por auténticos hackers, sin obtener los resultados que pretendía; incluso llegando a perjudicarse a él mismo.

***LAN:*** Abreviatura de Local Area Network (Red de Área Local o simplemente Red Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

***Log:*** Registro, en inglés. Muchos programas y sistemas crean distintos ficheros de registro en los que van anotando los pasos que dan (lo que hace un cierto usuario, como transcurre una conexión, etc).

***Malware:*** Es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño. Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de softwares o programas de códigos hostiles e intrusivos.

***MS-DOS:*** MS-DOS son las siglas de Microsoft Disk Operating System, Sistema operativo de disco de Microsoft. es un sistema operativo comercializado por Microsoft perteneciente a la familia DOS.

***P2P:*** Se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red.

***Pharming:*** Se basa en la manipulación de la información DNS con el objetivo de desviar tráfico destinado a websites legítimos, hacia websites fraudulentos desde los que perpetrar el fraude.

***Phishing:*** Es un tipo de estafa electrónica cuyo objetivo es el robo de datos de índole personal, con la finalidad de obtener beneficios económicos directos o indirectos para quienes lo llevan a cabo. El tipo de información que se intenta conseguir al perpetrar este tipo de estafas se centra

fundamentalmente en datos financieros, pero también incluye toda clase de credenciales (usuario y contraseña) de websites de diversa índole y otro tipo de datos personales.

***Rootkits y backdoors:*** Son códigos maliciosos que elaboran metodologías para permitir el acceso a un ordenador. Van desde los más simples (un programa escuchando en un puerto determinado) hasta los más complejos (un programa que esconderá sus procesos en memoria, modificará los archivos de registros y escuchará en un puerto). A menudo un backdoor será tan simple como crear un usuario que tiene privilegios de super-usuario con la esperanza de que no se note. Esto se debe porque un backdoor está diseñado para evitar el control normal de autenticación de un sistema.

***SAN:*** Una red de área de almacenamiento, en inglés SAN (Storage Area Network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de respaldo principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y confiable los distintos elementos que la conforman.

***Sniffing:*** Supone una amenaza grave para la seguridad no sólo de una máquina sino también de toda una red. Lamentablemente, una gran cantidad de tráfico confidencial viaja en claro, sin ningún tipo de cifrado, por las redes de la mayoría de las empresas.

***Software defectuoso (bugs):*** Es todo error en la programación, que impide funcionar bien a los equipos de cómputo, se le llama así por la entrada de una polilla en una computadora que funcionaba a base de válvulas de vacío, lo cual impedía su actividad.

***Spam:*** Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

***Spammers:*** Es una persona o bot que se dedica a la distribución y/o presentación de spam (correo o mensajes considerados basura).

***Spoofing:*** Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

***Spyware:*** Es código que se instala clandestinamente casi siempre de sitios de Internet que puedas visitar. Una vez instalado buscará en tu ordenador información que considere de valor. Esto podrán ser o estadísticas de tu utilización de Internet o hasta tu número de tarjeta de crédito. Algunas versiones de Spyware inadvertidamente se dan a conocer porque hacen aparecer avisos en tu escritorio de manera irritante.

***SSH:*** Nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

***Sun3:*** Sun-3 fue el nombre dado a una serie de estaciones de trabajo y servidores UNIX producidos por Sun Microsystems, lanzado en 1985.

***TCP/IP:*** La familia de protocolos de Internet (TCP/IP) es un conjunto de protocolos de red que implementa la pila de protocolos en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

***Token:*** Un token de seguridad (también llamado token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

***Troyano:*** Los Troyanos son códigos maliciosos que intentan mostrarse como algo útil o apetecible para que uno lo ejecute. Una vez ejecutados intentarán instalar un backdoor o rootkit, o aún peor, intentarán marcar un número de teléfono de acceso a Internet de alto coste, lo que te costará mucho dinero.

***Unix:*** Sistema operativo portable, multitarea y multiusuario; desarrollado en principio por un grupo de empleados de los laboratorios Bell de AT&T. Desde el punto de vista técnico, UNIX se refiere a una familia de sistemas operativos que comparten unos criterios de diseño e interoperabilidad en común. Esta familia incluye más de 100 sistemas operativos desarrollados a lo largo de 20 años.

***VAX:*** Máquina CISC sucesora de la PDP-11, producida por Digital Equipment Corporation. Su nombre original era VAX-11 (Virtual Address Extended PDP-11). Lanzada el 25 de octubre de 1977, fue la primera máquina comercial de arquitectura de 32 bits, lo que la convierte en un hito destacable en la historia de la computación. La primera VAX-11/780 fue instalada en Carnegie Mellon University

Su sistema operativo, VMS (luego llamado OpenVMS), fue concebido junto con la máquina. Presentaba características muy novedosas para su tiempo, en particular un revolucionario sistema de *clustering*

***Virus:*** Son programas auto replicantes que al igual que un virus biológico se adjuntan a otro programa, o en el caso de virus “macro” se adjuntan a otro archivo. El virus se ejecuta solamente cuando se ejecuta el programa o se abre el archivo infectado. Esto es lo que diferencia a los virus de los gusanos: si no se accede al programa o archivo entonces el virus no se ejecutará y por lo tanto no se replicará.

***Zombi:*** Computadoras que tras haber sido infectadas por algún tipo de malware, pueden ser usadas por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo.

# CAPÍTULO IV

# 4. METODOLOGIA DE LA INVESTIGACIÓN

## 4.1 Estado del Arte: Modelos de Investigación Existentes

### 4.1.1 Evaluación del Riesgo

El objetivo de la evaluación del riesgo es identificar los riesgos a los cuales están expuestos los activos de información de las organizaciones. Los riesgos son la función de los valores de los activos en riesgo, la probabilidad de ocurrencia de las amenazas que causan impacto en el negocio, la facilidad de la explotación de las vulnerabilidades por las amenazas identificadas y cualquier control existente o planeado que pudiera reducir los riesgos.

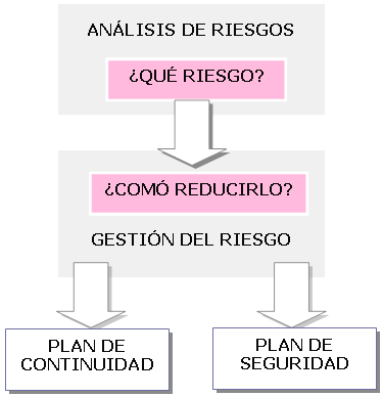



**Gráfico Nº 17 – Análisis de Riesgos**

La organización se propone reducir los factores del riesgo de todos sus activos de información a un nivel aceptable, de tal modo que el negocio crítico no sea afectado. En todo momento quedará un "Nivel del Riesgo"

que es "el Nivel Aceptable del Riesgo" como sea fijado por la administración. "El Riesgo aceptable es el nivel del riesgo que la administración esta preparada a aceptar como riesgo del negocio".

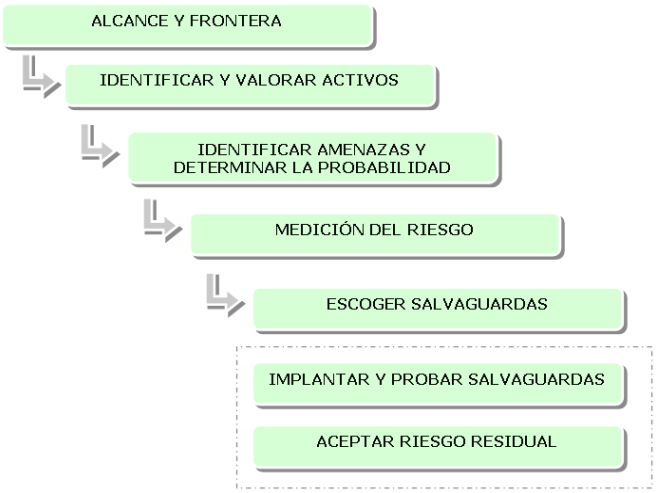



**Gráfico Nº 18 – Esquema de los Siete Procesos**

### 4.1.2 Los 7 Procesos

**Proceso 1 - Definir el Alcance y la Frontera**

Este proceso determina la dirección que la gestión de riesgos tomará. Define cuánto de la LAN (la frontera) y en cuánto detalle (el alcance) el proceso de la gestión de riesgos abarcará. La frontera definirá aquellas partes que serán consideradas. La frontera puede incluir su totalidad o partes de ella, tal como la función de comunicaciones de datos, la función de servidor, las aplicaciones, etc. Los factores que determinan la frontera pueden estar basados en la propiedad, la administración o el control. Colocar la frontera alrededor de una parte de la LAN controlada puede traer como resultado problemas de cooperación que pueden llevar a resultados inexactos. Este problema enfatiza la necesidad de la cooperación entre aquellos involucrados con la propiedad y la

administración de las diferentes partes, así como las aplicaciones y la información procesadas en esta.

El alcance de la gestión de riesgos también debe ser definido. Este puede ser pensado como un esquema lógico que muestra, dentro de la frontera, la profundidad del proceso de la gestión de riesgos. Lo distinguen las diferentes áreas de la LAN (dentro de la frontera) y los diferentes niveles de detalle utilizado durante el proceso de la gestión de riesgos. Por ejemplo algunas áreas pueden ser consideradas en un nivel más alto o más amplio, mientras que otras áreas pueden ser tratadas a fondo y con un enfoque limitado.

Para LAN más pequeñas, la frontera puede ser la red completa, y el alcance puede definir un nivel coherente de detalle de toda la red. Para LAN más grandes, una organización puede decidir colocar la frontera alrededor de aquellas áreas que ésta controla y definir el alcance para considerar todas las áreas dentro de la frontera. Sin embargo el enfocarse en comunicaciones de datos, conexiones externas, y ciertas aplicaciones quizás sea más limitado. Los cambios en la configuración, la adición de conexiones externas, o actualizaciones o mejoras al software de LAN o las aplicaciones pueden influir en el alcance.

**Proceso 2 - Identificar y Valorar los Activos**

La valoración de los activos identifica y asigna un valor a los activos. Todas las partes de la LAN tienen un valor aunque algunos activos definitivamente tienen más valor que otros. Este paso da la primera

indicación de aquellas áreas donde se debe prestar la mayor atención. Para LANs que producen grandes cantidades de información que no pueden ser analizadas razonablemente, puede necesitar que se realice una investigación inicial. Definir y valorar los activos pueden permitir a la organización decidir inicialmente que áreas pueden ser filtradas y que áreas deben ser señaladas con prioridad alta.

Diferentes métodos pueden ser utilizados para identificar y valorar los activos. La metodología del riesgo que una organización escoge puede proporcionar la guía en la identificación de los activos y debe proporcionar una técnica para valorarlos. Generalmente los activos pueden ser valorados basados en el impacto y las consecuencias para la organización. Esto incluiría no sólo el costo de sustitución del activo, sino que también el efecto en la organización si el activo es revelado, modificado, destruido o maltratado en cualquier otra manera.

Debido a que el valor de un activo debe basarse en más que sólo el costo de sustitución, la valoración de activos es uno de los procesos más subjetivos. Sin embargo, si la valoración del activo se realiza con la meta del proceso en mente, esto es, para definir los activos en términos de una jerarquía de importancia o criticidad, la relación de los activos llega a ser más importante que la colocación de un valor "correcto" en ellos.

La metodología de la evaluación del riesgo debe definir la representación de los valores de los activos. Las metodologías puramente cuantitativas pueden utilizar valores monetarios. Sin embargo teniendo que colocar un

valor monetario en algunas de las consecuencias que pueden ocurrir en los entornos de hoy puede ser suficiente para cambiar la percepción del proceso de la gestión de riesgos de ser desafiante a ser inconsecuente.

Muchas metodologías de la evaluación del riesgo en uso actualmente requieren la valoración de los activos en términos más cualitativos. Mientras que este tipo de valoración puede ser considerado más subjetivo que un enfoque cuantitativo, si la escala usada para valorar los activos es utilizada coherentemente a través del proceso de gestión de riesgos, los resultados producidos deberían ser útiles. A lo largo del presente trabajo del proceso de la gestión de riesgos, se presentará una técnica sencilla para valorar los activos, determinando la medida del riesgo, estimando el costo de la salvaguarda, y determinando la mitigación del riesgo. Esta técnica es sencilla y aún valida; será utilizada en el presente trabajo para mostrar la relación entre los procesos implicados en la gestión de riesgos.

Uno de los resultados implícitos de este proceso es una configuración detallada de la LAN, así como sus usos. Esta configuración debe indicar el hardware incorporado, las aplicaciones de software de mayor uso, información significativa procesada, así como “cómo la información fluye”. El grado de conocimiento de la configuración dependerá de la frontera y el alcance definidos.

Después de que la configuración de LAN sea completada, y los activos sean determinados y valorados, la organización debe tener una vista

razonablemente correcta de lo que contiene y qué áreas necesitan ser protegidas.

**Proceso 3 - Identificar las Amenazas y Determinar la Probabilidad**

El resultado de este proceso debe ser un fuerte indicador de las acciones adversas que podrían dañar la LAN, la probabilidad que estas acciones puedan ocurrir, y las debilidades que pueden ser explotadas para causar la acción adversa. Para alcanzar este resultado, las amenazas y vulnerabilidades necesitan ser identificadas y la probabilidad que una amenaza ocurra necesita ser determinada.

Existen grandes cantidades de información en la variedad de amenazas y vulnerabilidades. Algunas metodologías de la gestión de riesgos proporcionan también información en posibles amenazas y vulnerabilidades, así como la experiencia del usuario y la experiencia de la administración.

El grado de cuales amenazas son consideradas dependerá de la frontera y el alcance definidos para el proceso de la gestión de riesgos. Un análisis de alto nivel puede señalar amenazas y vulnerabilidades en términos generales; un análisis más enfocado puede vincular una amenaza a un componente específico o uso de la LAN. Por ejemplo un análisis de alto nivel puede indicar que la consecuencia debido a la pérdida de confidencialidad de datos por la revelación de información en la LAN es un riesgo demasiado grande. Un análisis un poco más enfocado puede indicar que la consecuencia debido a la revelación de

datos personales capturados y leídos a través de la transmisión de LAN es un riesgo demasiado grande. Más que probable, la generalidad de las amenazas producidas en el análisis de alto nivel, al final, produce las recomendaciones de salvaguarda que serán también de alto nivel. Esto es aceptable si la evaluación del riesgo fue definida en un alto nivel. La evaluación más estrechamente enfocada producirá una salvaguarda que puede reducir específicamente un riesgo dado, tal como la revelación de datos personales.

Las amenazas y vulnerabilidades deben ser expuestas cuando sean encontradas. Cualquiera de los activos de la LAN que fuera determinado a ser lo suficientemente importante (es decir, no fue filtrado por el proceso de investigación) debe ser examinado para determinar aquellas amenazas que podrían dañarla potencialmente. Para una evaluación más enfocada, se debe prestar particular atención para detallar las maneras que estas amenazas podrían ocurrir. Por ejemplo, métodos de ataque que tiene como resultado el acceso no autorizado pueden ser un repetitivo inicio de sesión, crackeo de contraseñas, adición de un equipo no autorizado a la red, etc. Estas especificaciones proporcionan más información en la determinación de vulnerabilidades y proporcionarán más información para proponer salvaguardas.

Este proceso puede descubrir algunas vulnerabilidades que pueden ser corregidas mejorando la administración y controles operacionales inmediatamente. Estos controles mejorados reducirán el riesgo de la amenaza en algún grado, hasta el momento en que más mejoras sean

completadas, planeadas e implementadas. Por ejemplo, aumentando la longitud y la composición de la contraseña para la autenticación puede ser una manera para reducir la vulnerabilidad de adivinar las contraseñas. Utilizar contraseñas más robustas es una medida que puede ser aplicada rápidamente para aumentar la seguridad. Al mismo tiempo, la planificación y la implementación de un mecanismo más avanzado de autenticación pueden acontecer.

Los controles existentes de la seguridad informática deben ser analizados para determinar si ellos proporcionan actualmente la protección adecuada. Estos controles pueden ser técnicos, procesales, etc. Si un control no proporciona la protección adecuada, puede ser considerado una vulnerabilidad. Por ejemplo, un sistema operativo puede proporcionar control de acceso a nivel de directorio, antes que a nivel de archivo. Para algunos usuarios, la amenaza de transigir la información puede ser demasiado grande el no tener protección a nivel de archivo. En este ejemplo, la falta de granularidad en el control del acceso podría ser considerada una vulnerabilidad.

Como las amenazas específicas y las vulnerabilidades relacionadas están identificadas, se necesita de la medida de la probabilidad asociada con el par amenaza/vulnerabilidad (por lo tanto, cual es la probabilidad de que se materialice una amenaza, dado que la vulnerabilidad es explotada?). La metodología del riesgo escogida por la organización debe proporcionar la técnica usada para medir la probabilidad. Junto con la valoración del activo, la asignación de medidas de probabilidad puede

ser también un proceso subjetivo. Los datos de la amenaza para amenazas tradicionales (mayormente amenazas físicas) existen y pueden ayudar en la determinación de la probabilidad. Sin embargo la experiencia con respecto a los aspectos técnicos y el conocimiento de los aspectos operacionales de la organización pueden demostrar ser más valiosos para decidir la medida de la probabilidad. Aunque la valoración del activo y las medidas de la probabilidad proporcionados en este ejemplo parecen ser de igual peso para cada par de amenaza/vulnerabilidad, es la determinación del usuario con respecto a cuales medidas deben ser acentuadas durante el proceso de la medida del riesgo.

**Proceso 4 – La Medición del Riesgo**

En su sentido más amplio la medida del riesgo puede ser considerada la representación de las clases de acciones adversas que pueden sucederle a un sistema o la organización y el grado de probabilidad que estas acciones puedan ocurrir. El resultado de este proceso debe indicar a la organización el grado del riesgo asociado a los activos definidos. Este resultado es importante porque es la base para hacer la selección de las salvaguardas y de las decisiones de mitigación de riesgo. Hay muchas maneras de medir y representar el riesgo. "A Framework for Computer Security Risk Management" [KATZ92] [10] indica que dependiendo de la metodología o el enfoque particular, la medida podría ser definida en términos cualitativos, términos cuantitativos, de una

[10] [KATZ92] Katzke, Stuart W. ,Phd., "A Framework for Computer Security Risk Management", NIST, Octubre, 1992.

dimensión, multidimensional, o alguna combinación de éstos. El proceso de la medida del riesgo debe ser consecuente con (y más que probablemente definido por) la metodología de la evaluación del riesgo para ser utilizada por la organización. Los enfoques cuantitativos a menudo son asociados con la medición del riesgo en términos de pérdidas monetarias. Los enfoques cualitativos a menudo son asociados con la medición el riesgo en términos de calidad como se indica a través de una escala o ranking. Un enfoque dimensional sólo considera componentes limitados (por ejemplo, el riesgo = la magnitud de la pérdida X la frecuencia de la pérdida). Los enfoques multidimensionales consideran componentes adicionales en la medida del riesgo tal como la certeza, la seguridad, o el desempeño. Uno de los aspectos más importantes de la medida del riesgo es que la representación es entendible y significativa para los que necesitan hacer la selección de la salvaguarda y las decisiones de mitigación de riesgo.

La comparación de medidas de riesgo debe tener en cuenta la criticidad de los componentes usados para determinar la medida del riesgo. Para las metodologías sencillas que sólo miran la pérdida y la probabilidad, una medida del riesgo que fue derivada de una pérdida alta y probabilidad baja puede tener como resultado la misma medida del riesgo como uno que resultó de una pérdida baja y probabilidad alta. En estos casos, el usuario necesita decidir cuál medida del riesgo considera más crítico, aunque las medidas del riesgo puedan ser iguales. En este caso, un usuario puede decidir que la medida del riesgo derivada de la

alta pérdida es más crítica que la medida del riesgo derivado de la probabilidad alta. Con una lista de posibles amenazas, vulnerabilidades y riesgos relacionados, una evaluación de la situación actual de la seguridad puede ser determinada. Las áreas que tienen una protección adecuada no surgirán contribuyendo como un riesgo (de modo que una protección adecuada debe llevar a una probabilidad baja) mientras que aquellas áreas que tienen una protección más débil surgen necesitando atención.

**Proceso 5 – Escoger las Salvaguardas Apropiadas**

El propósito de este proceso es de escoger salvaguardas apropiadas. Este proceso puede ser hecho utilizando la prueba de aceptación del riesgo.

La prueba de aceptación del riesgo es descrita por [KATZ92] como una actividad que compara la medida actual del riesgo con criterios de aceptación y resultado en una determinación de si el nivel actual del riesgo es aceptable. Mientras las consideraciones efectivas de la seguridad y el costo son los factores importantes, es posible que haya otros factores para considerar tal como: la política de la organización, la legislación y la regulación, los requisitos de la seguridad y la certeza, los requisitos del desempeño, y los requisitos técnicos.

La relación entre la prueba de aceptación del riesgo y la selección de salvaguardas puede ser iterativa. Inicialmente, la organización necesita ordenar los niveles diferentes del riesgo que fueron determinados

durante la evaluación del riesgo. Junto con estas la organización necesita decidir la cantidad de riesgo residual que estará dispuesto a aceptar después de que las salvaguardas escogidas sean aplicadas. Estas decisiones iniciales de aceptación del riesgo pueden ser tenidas en cuenta en la ecuación de la selección de salvaguarda. Cuándo las propiedades de las salvaguardas candidatas son conocidas, la organización puede reconsiderar las medidas de la prueba de la aceptación del riesgo y determinar si el riesgo residual es alcanzado, o altera la decisión de la aceptación del riesgo para reflejar las propiedades conocidas de las salvaguardas. Por ejemplo puede que haya riesgos que sean determinados a ser demasiado altos. Sin embargo después de revisar las salvaguardas disponibles, se puede verificar que las soluciones actuales ofrecidas son muy costosas y no pueden ser aplicadas fácilmente en la actual configuración y software de red. Esto puede forzar a la organización a gastar recursos para reducir el riesgo, o decidirse por la aceptación del riesgo porque es actualmente demasiado costoso mitigarlo.

Muchas fuentes existen que puedan proporcionar información sobre potenciales salvaguardas. La metodología discutida aquí define salvaguardas en términos de servicios de seguridad y mecanismos. Un servicio de seguridad es la suma de mecanismos, procedimientos, etc. que son aplicados para proporcionar protección. Los servicios de seguridad deben estar relacionados con las amenazas definidas en la evaluación del riesgo.

En la mayoría de los casos la necesidad por un servicio específico debe ser obvia fácilmente. Si los resultados de la aceptación del riesgo indican que un riesgo es aceptable, (es decir, los mecanismos existentes son adecuados) entonces no hay necesidad de aplicar mecanismos adicionales al servicio que ya existe.

Después de que los servicios de seguridad necesitados sean determinados, considere la lista de mecanismos de seguridad para cada servicio. Para cada servicio de seguridad escogido, determine los mecanismos candidatos que proporcionarían mejor ese servicio. Utilizando la relación amenaza/vulnerabilidad/riesgo desarrollado en los procesos previos, escoger aquellos mecanismos que potencialmente podrían reducir o eliminar la vulnerabilidad y así reducir el riesgo de la amenaza. En muchos casos, una relación de amenaza/vulnerabilidad producirá más de un mecanismo candidato. Por ejemplo la vulnerabilidad de utilizar contraseñas débiles podría ser reducida utilizando un mecanismo generador de contraseñas, utilizando un mecanismo basado en tokens, etc. Escoger los mecanismos candidatos es un proceso subjetivo que variará de una implementación de LAN a otra.

Escoger las apropiadas salvaguardas es un proceso subjetivo. Cuando se considera la medida del costo del mecanismo, es importante que el costo de la salvaguarda este relacionado a la medida del riesgo para determinar si la salvaguarda será rentable. La metodología escogida por la organización debe proporcionar una medida para representar que los

costos sean consecuentes con las medidas utilizadas para representar las otras variables determinadas hasta ahora.

Cuándo una medida (o costo) es asignado a la salvaguarda, puede ser comparado a otras medidas en el proceso. La medida de la salvaguarda puede ser comparada a la medida del riesgo (si este consiste en un valor) o los componentes de la medida del riesgo. Hay diferentes maneras de comparar la medida de la salvaguarda a la medida del riesgo. La metodología de la gestión de riesgos escogida por la organización debe proporcionar un método para seleccionar esas salvaguardas efectivas que reducirán el riesgo de la LAN a un nivel aceptable.

**Proceso 6 – Implementar y Probar las Salvaguardas**

La implementación y prueba de las salvaguardas deben hacerse de una manera estructurada. La meta de este proceso es asegurar que las salvaguardas sean aplicadas correctamente, sean compatibles con otras funcionalidades y salvaguardas, y proporcionen la protección esperada. Este proceso empieza desarrollando un plan para la implementación de salvaguardas. Este plan debe considerar los factores tales como financiación disponible, el proceso de aprendizaje de los usuarios, etc. Un plan de prueba para cada salvaguarda debe ser incorporado en este plan, y debe mostrar como cada interactúan o afectan a otras salvaguardas (o a los mecanismos de alguna otra funcionalidad). Los resultados esperados (o la suposición de ningún conflicto) de la interacción debe ser detallado. Debe reconocerse que no sólo es

importante que la salvaguarda se desempeñe funcionalmente como se esperaba y proporcione las protecciones esperadas, sino que esta no contribuya al riesgo por un conflicto con alguna otra salvaguarda o funcionalidad.

Cada salvaguarda debe ser probada primero independientemente de otras para asegurarse que esta proporcione la protección esperada. Esto puede no ser relevante si la salvaguarda esta diseñada para interactuar con otras salvaguardas. Después de probar la salvaguarda independientemente, esta debe ser probada con otras salvaguardas para asegurar que no interrumpa el normal funcionamiento de aquellas existentes. El plan de implementación debe justificar todas estas pruebas y debe reflejar cualquier problema o condiciones especiales como consecuencia de la prueba.

**Proceso 7 - Aceptar el Riesgo Residual**

Después de que todas las salvaguardas sean aplicadas, probadas y encontradas aceptables, los resultados de la prueba de aceptación del riesgo deben ser reconsiderados. El riesgo asociado con la relación de amenaza/vulnerabilidad ahora debería ser reducido a un nivel aceptable o eliminado. Si este no es el caso, entonces las decisiones hechas en los pasos previos deben ser reconsideradas para determinar como debe ser una protección apropiada.

## 4.2 Metodología : Análisis de Riesgos

### 4.2.1 Recursos a Proteger

Se presentan los distintos activos reconocidos en la Universidad, asignando un valor a la importancia que tienen en la institución, ponderada en una escala del 1 al 10. Esta importancia es un valor subjetivo que refleja el nivel de impacto que puede tener la institución si un incidente afecta a los activos, sin considerar las medidas de seguridad que existan sobre los mismos.

| ACTIVO | IMPORTANCIA |
|---|---|
| Base de Datos | 10 |
| Servidores | 10 |
| Sistema de correo | 10 |
| Sistema de almacenamiento (SAN) | 10 |
| Central de Telefonía IP y teléfonos IP | 10 |
| Copias de respaldo | 9 |
| Equipos de comunicación (Routers, switches, hubs, etc) | 9 |
| Equipos de seguridad (antivirus, antispam, antipishing, detección de intrusos, cortafuego) | 8 |
| Cableado de fibra óptica y par trenzado (UTP) | 8 |
| Código fuente de las aplicaciones | 8 |
| Equipo de respaldo (backups) | 7 |
| Administrador de TI | 7 |
| Usuarios | 5 |
| Hardware | 3 |
| Insumos | 2 |
| Documentación | 2 |
| Datos del usuario | 1 |

**Tabla Nº 1 – Identificación y Valoración de Activos**

### 4.2.2 Clases de Amenazas

Se clasificarán las amenazas en cinco clases principales: develación, interrupción, modificación, destrucción y eliminación o pérdida.

| Clase de Amenaza | Definición |
|---|---|
| Develación | Los activos que tienen un alto requerimiento de *confidencialidad* son sensibles a la develación. Esta clase de amenaza compromete a los activos a la develación no autorizada de información sensible. |
| Interrupción | La interrupción se relaciona principalmente a los activos en servicio. La interrupción impacta en la *disponibilidad* del activo o servicio. Un corte de energía es un ejemplo de esta amenaza. |
| Modificación | El principal impacto de esta clase de amenaza es en el requerimiento de *integridad*. Recordar que la integridad incluye la certeza y completitud de la información. Un intento de hackeo puede caer en esta clase de amenaza si se llegan a realizar los cambios. |
| Destrucción | Una amenaza que destruye el activo, cae en la clase de destrucción. Un activo que tiene un requerimiento de alta *disponibilidad* es particularmente sensible a la destrucción. Amenazas como terremotos, inundaciones, incendios y vandalismo están dentro de esta clase. |
| Eliminación o Pérdida | Cuando un activo esta sujeto a robo o ha sido extraviado o perdido, el impacto es principalmente en la *confidencialidad* y *disponibilidad* del activo. Las laptops son particularmente vulnerables a esta amenaza. |

**Tabla Nº 2 – Clasificación de Amenazas**

### 4.2.3 Probabilidad de la Ocurrencia de la Amenaza

Se debe considerar, por activo, ambos el tipo de amenaza a la que puede estar sujeta el activo y la probabilidad de la amenaza. La probabilidad de la amenaza puede ser estimada de experiencias pasadas, de información sobre las amenazas proporcionada por las principales agencias y desde fuentes tales como otras organizaciones o servicios.

Los niveles de probabilidad de bajo, medio, y alto son usados de acuerdo a las siguientes definiciones:

| Nivel de Probabilidad | Definición |
|---|---|
| No Aplicable | Puede ser usado para indicar que una amenaza no es considerada relevante para la situación en revisión. |
| Bajo | No hay antecedentes y la amenaza esta considerada con poca probabilidad de ocurrencia. |
| Medio | Se tiene algún antecedente y una evaluación de que la amenaza pudiera suceder. |
| Alto | Se tiene un antecedente significativo y una evaluación de que la amenaza tiene una alta probabilidad de ocurrencia. |

**Tabla Nº 3 – Niveles de Probabilidad**

### 4.2.4 Nivel de Impacto

El impacto se define como el daño producido a la organización por un posible incidente y es el resultado de la agresión sobre el activo.

| Nivel de Impacto | Definición |
|---|---|
| Bajo | Indica pérdidas de información y/o recursos informáticos de nivel aceptable. |
| Medio | Indica pérdidas de información y/o recursos informáticos de nivel moderado. |
| Alto | Indica pérdidas de información y/o recursos informáticos de nivel severo hasta irrecuperable. |

**Tabla Nº 4 – Niveles de Impacto**

### 4.2.5 Factores de Riesgo

En los siguientes cuadros se listan los activos de la organización y los factores de riesgos identificados para cada caso, que los afectan directamente y las consecuencias que puede acarrear la ocurrencia de estos factores.

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| BASE DE DATOS | BD1 | Acceso no autorizado a datos (borrado, modificación, etc.) | Pérdida, revelación o modificación de datos; pérdida de tiempo y productividad | Un intruso accede a la base de datos | Modificación | B | A |
| | BD2 | Base de datos compleja | Desarrollo complejo de sistemas | Base de datos con alta densidad de registros o tablas | Interrupción | B | B |
| | BD3 | Copia no autorizada de un medio de datos | Divulgación de información | Un usuario accede a la base de datos y copia parte o toda la información | Develación | B | A |
| | BD4 | Errores de software | Inconsistencia en los datos | Falla en la aplicación de usuario | Interrupción | M | A |
| | BD5 | Falla de base de datos | Inconsistencia en los datos | Error o falla en el motor de base de datos | Interrupción | B | A |
| | BD6 | Falta de espacio de almacenamiento | Falla en la aplicación | Discos de baja capacidad de almacenamiento | Interrupción | B | M |
| | BD7 | Mala configuración de la programación de las copias de respaldo | Datos sin backup | Programación inadecuada en horario de producción | Modificación | M | M |
| | BD8 | Mala integridad de los datos | Inconsistencia y redundancia de datos | Base de datos diseñada o mantenida de forma deficiente lo cual provoca errores de integridad | Modificación | B | A |
| | BD9 | Medios de datos no están disponibles cuando son necesarios | Pérdida de tiempo y productividad | Base de datos diseñada o mantenida de forma deficiente lo cual provoca problemas de disponibilidad | Interrupción | B | A |
| | BD10 | Pérdida de copias de respaldo | Incapacidad de restauración | Falla en el hardware del equipo de respaldo | Pérdida | B | A |
| | BD11 | Perdida de confidencialidad en datos privados y de sistema | Divulgación de información | Exposición de información negligentemente | Develación | M | A |
| | BD12 | Perdida de datos en tránsito | Inconsistencia de datos y divulgación de información | Usuario malicioso conectado usando programas de intercepción | Pérdida | B | M |
| | BD13 | Portapapeles, impresoras o directorios compartidos | Divulgación de información | Impresión de un reporte | Develación | M | A |
| | BD14 | Robo | Pérdida de información | Sustracción del medio de almacenamiento | Pérdida | B | M |
| | BD15 | Sabotaje | Pérdida o modificación de datos, pérdida de tiempo y productividad | Ataque a la base de datos | Modificación | A | A |
| | BD16 | Seguridad de base de datos deficiente | Perdida o modificación de datos | Seguridad mínima en el servidor base de datos | Modificación | B | A |
| | BD17 | Spoofing y sniffing | Divulgación y modificación de información | Usuario malicioso conectado usando programas de intercepción | Develación | A | A |
| | BD18 | Transferencia de datos incorrectos | Inconsistencia de datos | Error de digitación | Modificación | M | M |
| | BD19 | Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Ingreso de virus vulnerando el sistema | Destrucción | M | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| SERVIDORES | SE1 | Acceso no autorizado a datos | Robo, modificación de información | Usuario accede a la información contenida en el servidor sin contar con los permisos necesarios | Develación | M | M |
| | SE2 | Acceso no autorizado a equipos | Robo, modificación de información | Usuario accede al servidor sin contar con los permisos necesarios | Develación | B | A |
| | SE3 | Corte de luz, UPS descargado o variaciones de voltaje | Falta de sistema | El suministro eléctrico sufre frecuentes interrupciones | Interrupción | B | A |
| | SE4 | Destrucción o mal funcionamiento de un componente | Pérdida de tiempo por necesidad de reemplazo | Falla del servidor de directorio | Interrupción | M | A |
| | SE5 | Error de configuración y operación | Aumento de vulnerabilidades e inestabilidad en el sistema | Controladores de disco mal instalados | Interrupción | B | A |
| | SE6 | Factores ambientales | Falta de sistema y destrucción de equipos | Equipo expuesto a un ambiente con un índice de humedad alto | Destrucción | B | A |
| | SE7 | Límite de vida útil - Máquinas obsoletas | Deterioro en la performance del sistema | Servidores adquiridos con una antigüedad superior a 5 años | Interrupción | M | A |
| | SE8 | Mal mantenimiento | Interrupciones en el funcionamiento del sistema | Condiciones de conservación y mantenimiento de los servidores inadecuadas | Interrupción | B | M |
| | SE9 | Modificación no autorizada de datos | Inconsistencia de datos, mala configuración, fraude | Usuario registrando datos indebidos | Modificación | B | M |
| | SE10 | Robo | Pérdida de equipamiento o información | Sustracción de servidores | Pérdida | B | A |
| | SE11 | Spoofing y sniffing | Divulgación, modificación y robo de información | Usuario malicioso conectado usando programas de intercepción | Develación | A | A |
| | SE12 | Virus, gusanos y caballos de Troya | Fallas generales del sistema y en la red | Un virus se ha introducido en el servidor | Destrucción | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| SISTEMA DE CORREO | SC1 | Cuentas de correo activas de ex - usuarios | Uso indebido del servicio | No se eliminan las cuentas de alumnos egresados o personal que deja de laborar | Develación | M | B |
| | SC2 | Errores en las funciones de encriptación | Divulgación de información (contraseñas) | Información fácil de decodificar | Develación | B | M |
| | SC3 | Falta de autenticación | Exposición de información | Configuración automática de los clientes de correo | Develación | M | A |
| | SC4 | Mal uso del servicio de correo | Disminución de la performance del ancho de banda | Envío de correo no deseado | Interrupción | M | A |
| | SC5 | Mala integridad de los datos | Inconsistencia de información | Clientes de correo dañados | Modificación | B | M |
| | SC6 | Perdida de confidencialidad en datos privados y de sistema | Divulgación de información | Dejar abierta la sesión al momento de ausentarse | Develación | M | A |
| | SC7 | Perdida de datos en tránsito | Pérdida de información | Falla de equipos intermedios | Pérdida | B | M |
| | SC8 | Sabotaje | Pérdida del servicio | Conflicto IP al servidor de correo | Interrupción | B | A |
| | SC9 | Spoofing y sniffing | Divulgación, modificación y robo de información | Usuario malicioso conectado usando programas de intercepción | Develación | M | A |
| | SC10 | Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Un virus se ha introducido en los buzones de los usuarios | Destrucción | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| SISTEMA DE ALMACENAMIENTO (SAN) | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | SA1 | Acceso no autorizado a equipos | Robo, modificación de información | Usuario accede a la SAN sin contar con los permisos necesarios | Modificación | B | A |
| | SA2 | Administración impropia del sistema | Modificación de datos, perdida de la configuración | Acción negligente del sistema de administración de la SAN | Modificación | B | A |
| | SA3 | Condiciones de trabajo adversas | Pérdida de datos, deterioro del equipo | Falta de un ambiente refrigerado y con voltaje regulado | Pérdida | B | A |
| | SA4 | Daño de cables inadvertido | Pérdida e interrupción de datos | Tendido de fibra entre los servidores y la SAN sin seguridad y de fácil acceso | Interrupción | B | A |
| | SA5 | Falla en la SAN | Pérdida de información, paralización del servicio | Mal funcionamiento de los discos de canal de fibra | Destrucción | B | A |
| | SA6 | Falla en medios externos | Pérdida de datos en medios externos | Deterioro del medio de almacenamiento | Perdida | B | A |
| | SA7 | Mala integridad de los datos | Inconsistencia de información | Falla en el sistema de redundancia | Modificación | B | A |
| | SA8 | Mantenimiento inadecuado o ausente | Perdida o deterioro de datos | Reducción de la vida útil del equipo sin un debido mantenimiento | Destrucción | M | A |
| | SA9 | Medios de datos no están disponibles cuando son necesarios | Pérdida de tiempo y productividad por falta de datos | Caída de medios de almacenamiento | Pérdida | B | A |
| | SA10 | Sabotaje | Pérdida o robo de información | Acceso indebido al sistema de administración | Pérdida | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| CENTRAL DE TELEFONÍA IP Y TELÉFONOS IP | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | CT1 | Acceso no autorizado a equipos | Robo, modificación de información | usuario accede a la central sin contar con los permisos necesarios | Modificación | B | A |
| | CT2 | Administración impropia del sistema | Modificación de datos, perdida de la configuración | Acción negligente sobre la central telefónica | Modificación | B | A |
| | CT3 | Ancho de banda insuficiente | Interrupción del servicio | Medios de transmisión saturados por aplicaciones multimedia | Interrupción | M | A |
| | CT4 | Conexiones de cables inadmisible | Interrupción del servicio | Uso de cables deteriorados u obsoletos | Interrupción | B | M |
| | CT5 | Conservación deficiente | Interrupción del servicio | Uso de equipo sin un mínimo cuidado de conservación | Destrucción | M | A |
| | CT6 | Factores ambientales | Interrupción del servicio | Exceso de humedad, exposición directa al sol | Destrucción | B | A |
| | CT7 | Interferencia | Perdida del servicio | Interferencia electromagnética | Interrupción | B | A |
| | CT8 | Mantenimiento inadecuado o ausente | Perdida o deterioro de equipos | Reducción de la vida útil del equipo sin una debido mantenimiento | Destrucción | M | A |
| | CT9 | Sabotaje | Interrupción del servicio | Daño físico a los equipos | Destrucción | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| COPIAS DE RESPALDO | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | CR1 | Accesos no autorizados al medio de almacenamiento | Perdida, alteración o revelación de información | Usuario accede a las copias de respaldo sin contar con los permisos necesarios para ello | Develación | B | M |
| | CR2 | Clasificación deficiente de medios | Pérdida de medios de almacenamiento o retrasos en su restauración | Mala gestión del mantenimiento de las copias de respaldo | Pérdida | B | M |
| | CR3 | Conservación deficiente | Problemas en la restauración de la información | Medidas deficientes para el almacenamiento y conservación de medios | Pérdida | B | M |
| | CR4 | Copia no autorizada de un medio de datos | Robo de información | Copias desde CDs, DVDs y/o cintas | Develación | M | M |
| | CR5 | Errores de respaldo | Problemas en la restauración de información | El proceso de realización de copias de respaldo sufre errores frecuentes | Pérdida | B | A |
| | CR6 | Falla en medios externos | Pérdida de datos en medios externos | Cartuchos para respaldo defectuosos | Pérdida | B | A |
| | CR7 | Fallos en la disponibilidad de medios | Pérdida de medios de almacenamiento o retrasos en su restauración | Problemas para la obtención de copias de respaldo cuando son necesarias | Interrupción | B | M |
| | CR8 | Pérdida de medios | Imposibilidad de restauración de información | Imposibilidad de encontrar un medio de almacenamiento | Pérdida | B | A |
| | CR9 | Robo | Pérdida de información, imposibilidad de restauración | Sustracción de copias de respaldo | Pérdida | B | A |
| | CR10 | Sabotaje | Pérdida o robo de información | Daño físico a los cartuchos de respaldo | Destrucción | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| EQUIPOS DE COMUNICACIÓN (ROUTERS, SWITCHES, HUBS, ETC) | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | EC1 | Abuso de puertos para el mantenimiento remoto | Posibles intrusiones y robo o divulgación de información | Puerto de administración vulnerable | Develación | M | A |
| | EC2 | Ancho de banda insuficiente | Ralentización de la transmisión de información | El ancho de banda empleado para las transmisiones es inferior al adecuado | Interrupción | A | A |
| | EC3 | Configuración inadecuada de componentes de red | Errores de transmisión, interrupción del servicio de red | Utilización de configuraciones básicas | Interrupción | B | M |
| | EC4 | Corte de luz, UPS descargado o variaciones de voltaje | Interrupción de las transmisiones | El suministro eléctrico sufre frecuentes interrupciones | Interrupción | B | A |
| | EC5 | Denegación de servicio | Interrupción de todos o algunos de los servicios de red | Saturación de acceso a un servicio | Interrupción | B | A |
| | EC6 | Errores de operación | Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades | Falta de experiencia en la operación del equipo | Interrupción | B | M |
| | EC7 | Falta de autenticación | Posibles intrusiones y robo o divulgación de información | Inapropiado nivel de seguridad | Develación | B | B |
| | EC8 | Límite de vida útil - Máquinas obsoletas | Uso deficiente del sistema | Los componentes de transmisión no son los idóneos para una transmisión óptima | Pérdida | M | A |
| | EC9 | Mantenimiento deficiente | Errores de transmisión, mal funcionamiento de la red | Mantenimiento inadecuado de los componentes de transmisión | Interrupción | B | M |
| | EC10 | Modificación de paquetes | Alteración de la información | Hacker en la red | Modificación | M | A |
| | EC11 | Penetración, intercepción o manipulación del medio de transporte | Robo de información | Acceso indebido al cableado estructurado o a los equipos de comunicación | Develación | M | M |
| | EC12 | Perdida de datos en tránsito | Divulgación de información | Intercepción de señales microondas | Develación | B | B |
| | EC13 | Robo | Interrupción de la transmisión, gastos de reposición | Sustracción de equipos de transmisión | Pérdida | B | A |
| | EC14 | Sabotaje | Red inaccesible | Interrupción del medio de transmisión | Interrupción | M | A |
| | EC15 | Sincronización de tiempo inadecuada | Inconsistencia en datos | Utilización de configuración por defecto | Pérdida | B | A |
| | EC16 | Spoofing y sniffing | Divulgación, modificación y robo de información | Usuario malicioso conectado usando programas de intercepción | Develación | M | A |
| | EC17 | Velocidad de transmisión insuficiente | Ralentización de la transmisión de información | La velocidad empleada para las transmisiones es inferior a la adecuada, exceso de usuarios | Interrupción | A | M |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| EQUIPOS DE SEGURIDAD | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | EQ1 | Acceso no autorizado a equipos | Robo, modificación de información | Usuario accede al equipo de seguridad sin contar con los permisos necesarios | Modificación | B | A |
| | EQ2 | Administración impropia del sistema | Modificación de datos, perdida de la configuración | Acción negligente sobre el equipo de seguridad | Modificación | B | A |
| | EQ3 | Complejidad de las configuraciones | Administración mas laboriosa | Configuraciones largas que causan lentitud en el equipo de seguridad | Interrupción | A | M |
| | EQ4 | Modificación de paquetes | Alteración de la información | Equipo en deterioro o falto de mantenimiento | Modificación | B | A |
| | EQ5 | Sabotaje | Pérdida o robo de información | Modificación de la configuración de seguridad | Interrupción | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| CABLEADO DE FIBRA ÓPTICA Y PAR TRENZADO (UTP) | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | CB1 | Abuso de puertos para el mantenimiento remoto | Posibles intrusiones y robo o divulgación de información | Falta de protección a los medios de transmisión | Develación | M | B |
| | CB2 | Ancho de banda insuficiente | Transmisión pesada en la red o imposibilidad de utilizar el sistema en línea | Incremento del uso de servicios multimedia | Interrupción | A | A |
| | CB3 | Ausencia o falta de segmentación | Tramos de red extensos y dificultades en la comunicación | Falta tendido de red en ubicaciones de difícil acceso | Interrupción | M | M |
| | CB4 | Complejidad en el diseño de las redes de sistemas de TI | Dificultad en la administración y en el mantenimiento | Tamaño de la red y variedad de topología | Interrupción | M | M |
| | CB5 | Conexión de cables inadmisible | Robo de datos, spoofing y sniffing | Cableado que no va de acuerdo con el estándar | Interrupción | B | B |
| | CB6 | Conexiones todavía activas | Intrusión de usuarios no autorizados al sistema | Puntos de red activos en ubicaciones de poca actividad | Develación | B | M |
| | CB7 | Daño o destrucción de cables o equipamiento inadvertido | Pinchaduras de cables, robo de datos, spoofing y sniffing | Descuido en obras civiles | Pérdida | B | M |
| | CB8 | Factores ambientales | Interferencias o daños de equipamiento | Medio de transmisión expuesto a un ambiente sin protección | Interrupción | B | M |
| | CB9 | Falla en la SAN | Una o más servidores incomunicados | Deterioro de la fibra óptica | Interrupción | B | A |
| | CB10 | Interferencias | Errores en los datos de transmisión o imposibilidad de utilizar los servicios en línea | Fuentes electromagnéticas en la ruta del cableado estructurado | Modificación | B | M |
| | CB11 | Límite de vida útil del cableado estructurado | Cableado obsoleto y deterioro de la comunicación | Cableado estructurado con una antigüedad superior a 5 años | Interrupción | M | M |
| | CB12 | Longitud de los cables de red excedida | Transmisión lenta o con interferencias, o imposibilidad de utilizar los servicios de red | Cableado que no va de acuerdo con el estándar | Interrupción | B | M |
| | CB13 | Mal mantenimiento | Errores de transmisión o interrupción del servicio de red | Mantenimiento realizado por un personal principiante | Interrupción | B | M |
| | CB14 | Penetración, intercepción o manipulación del medio de transporte | Robo de información | Realización de conexiones clandestinas | Develación | M | A |
| | CB15 | Perdida de datos en tránsito | Divulgación de información | Intercepción de señales en la red | Develación | B | A |
| | CB16 | Reducción de velocidad de transmisión | Pérdida de tiempo de los usuarios, o imposibilidad de utilizar los servicios de red | Incremento de usuarios conectados a la red | Interrupción | M | B |
| | CB17 | Riesgo por el personal de limpieza o personal externo | Daño en cables o equipos, interrupción del servicio | Ignorancia sobre sistemas de información por el personal de limpieza | Interrupción | B | A |
| | CB18 | Sabotaje | Pérdida o robo de información | Destrucción del cableado estructurado | Pérdida | B | A |
| | CB19 | Transporte inseguro de archivos | Divulgación de información | Falta de encriptación de la información | Develación | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| CÓDIGO FUENTE DE LAS APLICACIONES | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | CF1 | Acceso no autorizado a datos (borrado, modificación, etc.) | Modificación del software en desarrollo | Acceso no autorizado al área de desarrollo | Modificación | B | A |
| | CF2 | Aplicaciones obsoletas | Disminución de productividad, mayor sensibilidad a vulnerabilidades | Las aplicaciones empleadas no están actualizadas para aprovechar todo su potencial | Interrupción | B | B |
| | CF3 | Aplicaciones sin licencia | Multas y problemas con Software Legal | No contar con software debidamente licenciado para el desarrollo de aplicaciones | Interrupción | A | M |
| | CF4 | Conocimiento insuficiente de los documentos de requerimientos en el desarrollo | Sistema inestable y excesivo pedido de cambios | Mala definición de requerimientos | Interrupción | B | M |
| | CF5 | Error de configuración y operación | Mal funcionamiento de los sistemas | Mala definición de variables en las aplicaciones | Pérdida | B | M |
| | CF6 | Errores en las funciones de encriptación | Problemas en la recuperación de archivos encriptados o divulgación de información | No se toma en cuenta las medidas de seguridad en el desarrollo de aplicaciones | Destrucción | M | A |
| | CF7 | Falla del sistema | Falta de sistema y posibles demoras | Falta de documentación completa de toda la aplicación | Interrupción | B | A |
| | CF8 | Falta de compatibilidad | Datos erróneos e inestabilidad del sistema | Uso de diferentes versiones de software de desarrollo | Interrupción | B | B |
| | CF9 | Falta de confidencialidad | Divulgación de información | Divulgación de información fuera del área de desarrollo | Develación | M | M |
| | CF10 | Mala administración de control de acceso (salteo del login, etc.) | Divulgación y modificación de información | Toma de privilegios indebidos de acceso a la aplicación | Develación | B | A |
| | CF11 | Pérdida de código fuente | Divulgación de información | Deterioro del medio de almacenamiento | Develación | B | A |
| | CF12 | Poca adaptación a cambios del sistema | Sistema inestable y de difícil modificación | Cambio en los requerimientos de la aplicación | Interrupción | M | A |
| | CF13 | Prueba de software deficiente | Sistema poco confiable | No se cuenta con un entorno de pruebas previas a la puesta en producción | Pérdida | B | M |
| | CF14 | Software desactualizado | Probabilidad incremental de vulnerabilidades y virus | Software defectuoso explotado | Pérdida | B | M |
| | CF15 | Virus, gusanos y caballos de Troya | Inestabilidad y mal funcionamiento de sistemas | Modificación de los archivos en desarrollo por código malicioso | Interrupción | M | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| EQUIPO DE RESPALDO (BACKUPS) | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | ER1 | Conservación deficiente | Pérdida de información, imposibilidad de restauración | Medidas inadecuadas para la conservación de medios de almacenamiento | Pérdida | B | M |
| | ER2 | Copia no autorizada a un medio de datos | Robo de información | Copias desde CDs, DVDs y/o cintas | Develación | M | M |
| | ER3 | Errores de software | Error en la generación o en la copia de respaldo a medios externos | El proceso de realización de copias de respaldo sufre errores frecuentes | Pérdida | B | A |
| | ER4 | Falla en medios externos | Pérdida de copias de respaldo | Mala gestión del mantenimiento de las copias de respaldo | Pérdida | B | A |
| | ER5 | Falta de espacio de almacenamiento | Falla en la generación de copias de respaldo | Saturación de los cartuchos de respaldo | Pérdida | M | A |
| | ER6 | Mala configuración de la programación de las copias de respaldo | Falta de copias de respaldo de datos | Proceso de backup en horas de producción | Interrupción | B | M |
| | ER7 | Mala integridad de los datos resguardados | Errores durante la restauración de datos | Falla en el hardware del equipo de respaldo | Pérdida | B | A |
| | ER8 | Medios de datos no están disponibles cuando son necesarios | Pérdida de copias de respaldo y retraso del sistema | Problemas para la obtención de copias de respaldo cuando son necesarias | Interrupción | B | A |
| | ER9 | Pérdida de copias de respaldo | Falta de datos, incapacidad de restaurarlos y divulgación de información | Imposibilidad de encontrar un medio de almacenamiento | Pérdida | B | M |
| | ER10 | Robo | Incapacidad de restaurarlos y divulgación de información | Sustracción del equipo de respaldo | Pérdida | B | A |
| | ER11 | Rótulos inadecuado en los medios de datos | Errores durante la restauración de datos | Descripción de los cartuchos ineficientemente | Pérdida | B | M |
| | ER12 | Sabotaje | Pérdida o robo de información | Destrucción del equipo de respaldo | Pérdida | B | A |
| | ER13 | Spoofing y sniffing | Divulgación, modificación y robo de información | Usuario malicioso conectado usando programas de intercepción | Develación | M | M |
| | ER14 | Virus, gusanos y caballos de Troya | Pérdida de datos de copias de respaldo | Un virus se ha almacenado en el medio de respaldo junto con los datos | Destrucción | M | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| ADMINISTRADOR DE TI | AT1 | Administración impropia del sistema de IT (responsabilidades y roles del personal de sistemas) | Asignación de responsabilidades impropia | No contar con el Cuadro de Asignación de Personal - CAP ni el Manual de Operaciones y Funciones - MOF | Modificación | B | B |
| | AT2 | Almacenamiento de contraseñas negligente | Divulgación de contraseñas y uso indebido de derechos de usuarios | Guardar las contraseñas en post-it | Develación | M | A |
| | AT3 | Configuración impropia del Postfix | Divulgación de mensajes, uso del servidor para enviar SPAM, fallas en la administración de cuotas de discos | Personal no capacitado | Develación | B | A |
| | AT4 | Errores de configuración y operación del sistema | Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades | Personal no capacitado | Interrupción | B | A |
| | AT5 | Falta de auditorías en sistemas informáticos | Imposibilidad del seguimiento de usuarios y de la generación de reportes | Limitación de tiempo y falta de aplicaciones para auditar | Interrupción | A | M |
| | AT6 | Mala evaluación de datos de auditoría | No se analizan los logs y por lo tanto no hay evaluación de los resultados | Limitación de tiempo y falta de aplicaciones para auditar | Interrupción | A | B |
| | AT7 | Mal uso de derechos de administrador | Mala distribución de los permisos y de las cuentas de administrador | Delegación de funciones de forma indebida | Modificación | M | M |
| | AT8 | Uso de derechos sin autorización | Robo de información | Acceso al sistema fuera del horario de trabajo | Develación | B | A |
| | AT9 | Uso impropio del sistema de IT | Administración deficiente | Abuso de privilegios por el personal de TI | Modificación | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| USUARIOS | US1 | Acceso no autorizado a datos | Divulgación o robo de información | Un usuario accede a datos a los cuales no está autorizado | Develación | B | A |
| | US2 | Borrado, modificación o revelación desautorizada o inadvertida de información | Inconsistencia de datos o datos faltantes | Un usuario provoca una pérdida o alteración de los datos existentes | Pérdida | M | A |
| | US3 | Condiciones de trabajo adversas | Predisposición a distracción, bajo rendimiento de usuarios | El espacio de trabajo no reúne las debidas condiciones para un desarrollo óptimo de las actividades | Interrupción | M | A |
| | US4 | Destrucción de un componente de hardware | Pérdida de tiempo por necesidad de reemplazo | Uso inapropiado de un equipo | Destrucción | B | M |
| | US5 | Destrucción negligente de datos | Pérdida de información | Alteración de datos por desconocimiento o negligencia | Pérdida | M | M |
| | US6 | Desvinculación del personal | Robo o modificación de información, sabotaje interno | Los procedimientos asociados a la baja de un empleado no son los adecuados | Develación | M | M |
| | US7 | Documentación deficiente | Mayor probabilidad de errores por falta de instrucciones | Los procedimientos de trabajo no se encuentran debidamente detallados | Interrupción | M | B |
| | US8 | Entrada sin autorización a los ambientes | Robo de equipos o insumos, divulgación de datos | Falta de control en el acceso de personas externas | Develación | M | M |
| | US9 | Entrenamiento de usuarios inadecuado | Predisposición a errores y bajo rendimiento de usuarios | La formación y entrenamiento del personal no es el adecuado | Interrupción | A | M |
| | US10 | Errores en el control de permisos y privilegios | Robo de información | El control de permisos y privilegios no es llevado con el debido rigor | Develación | M | A |
| | US11 | Falta de auditorías | Predisposición a un rendimiento mediocre y falta de concienciación sobre responsabilidades y seguridad | No se cuenta con una medida del rendimiento del uso del sistema | Pérdida | A | M |
| | US12 | Falta de cuidado en el manejo de la información (Ej. Contraseña) | Divulgación de datos | Contraseñas en post-it | Develación | M | A |
| | US13 | Ingeniería social - Ingeniería social inversa | Robo o modificación de información | Un usuario divulga datos confidenciales a personas no autorizadas | Develación | M | A |
| | US14 | Mal uso de derechos de administrador (sesiones abiertas) | Divulgación o robo de información, sabotaje interno | Violación a la privacidad de los usuarios y alteración de datos | Develación | B | A |
| | US15 | No-cumplimiento con las medidas de seguridad del sistema | Medidas correctivas tomadas por la gerencia, según la gravedad del incidente | Fácil acceso a hacker's a la violación del sistema | Modificación | B | A |
| | US16 | Pérdida de confidencialidad o integridad de datos como resultado de un error humano | Error en la información | Trabajar mas de las horas debidas, problemas ajenos a la institución | Modificación | B | A |
| | US17 | Problemas en el acceso físico a equipos | Respuesta tardía a evento | Un usuario tiene dificultades para acceder a su puesto de trabajo | Interrupción | M | A |
| | US18 | Uso descontrolado de recursos | Retraso en las actividades o falta de sistema | Malversación de recursos informáticos | Interrupción | B | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| HARDWARE | HD1 | Corte de luz, UPS descargado o variaciones de voltaje | Interrupción del funcionamiento de equipos | El suministro eléctrico sufre frecuentes interrupciones | Interrupción | B | M |
| | HD2 | Destrucción o mal funcionamiento de un componente | Interrupción de la tarea del usuario | Frecuentes errores en el desempeño de un equipo | Interrupción | B | M |
| | HD3 | Errores de funcionamiento | Interrupción/problemas en el funcionamiento del sistema | Frecuentes errores en el desempeño de un equipo | Interrupción | M | M |
| | HD4 | Factores ambientales | Destrucción o avería de equipos | Hardware expuesto al medio ambiente sin protección | Destrucción | B | A |
| | HD5 | Límite de vida útil | Avería de equipos | Equipos existentes demasiado anticuados para un funcionamiento óptimo | Interrupción | M | B |
| | HD6 | Mal mantenimiento | Avería de equipos e incremento en el costo de equipamiento de respaldo | El mantenimiento llevado a cabo sobre los elementos hardware no es el adecuado | Interrupción | B | A |
| | HD7 | Robo | Pérdida de equipamiento e interrupción de la tarea del usuario | Sustracción de equipos de hardware | Pérdida | B | M |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| INSUMOS | IN1 | Factores ambientales | Destrucción de insumos | Insumos expuestos al medio ambiente sin protección | Destrucción | B | A |
| | IN2 | Límite de vida útil | Destrucción o avería de los insumos | La caducidad o periodo de uso correcto de insumos no está debidamente controlado | Destrucción | B | M |
| | IN3 | Mala disponibilidad | Ralentización de las actividades | Los insumos no se encuentran disponibles cuando son necesarios | Interrupción | B | M |
| | IN4 | Malas condiciones de conservación | Destrucción o avería de los insumos | Las medidas de conservación de los insumos no son las adecuadas | Destrucción | M | A |
| | IN5 | Recursos escasos (recorte presupuestal) | Interrupción en el funcionamiento normal del sistema | Falta de presupuesto para la compra de insumos | Interrupción | M | A |
| | IN6 | Uso descontrolado de recursos | Incremento no justificado del gasto de insumos | El uso que se hace de los insumos no es el idóneo | Pérdida | B | M |
| | IN7 | Robo | Pérdida de insumos e incremento en el gasto | Sustracción de insumos | Pérdida | M | M |
| | IN8 | Transporte inseguro de insumos | Pérdida de insumos, e incremento en el gasto | Perdida o sustracción de insumos durante el transporte | Interrupción | B | B |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| DOCUMENTACIÓN | DO1 | Acceso no autorizado a datos de documentación | Divulgación, robo o modificación de información | Un usuario accede a la documentación sin estar autorizado para ello | Develación | B | M |
| | DO2 | Borrado o modificación desautorizada de información | Documentación incorrecta | Información sensible a un nivel bajo de seguridad | Modificación | B | M |
| | DO3 | Rebuscar información | Divulgación de información | Datos compartidos con bajo nivel de seguridad | Develación | B | A |
| | DO4 | Copia no autorizada de un medio de datos | Divulgación de información | Usuario que realiza una copia de información confidencial | Develación | M | M |
| | DO5 | Descripción de archivos inadecuada | Documentación incorrecta | La clasificación empleada para el almacenamiento de documentación no es la idónea | Interrupción | B | M |
| | DO6 | Destrucción negligente de datos | Documentación incorrecta | Ignorancia o negligencia del usuario | Destrucción | B | M |
| | DO7 | Documentación insuficiente o faltante, funciones no documentadas | Entorpecimiento de la administración y uso del sistema | La documentación existente es escasa en relación a las aplicaciones y equipos existentes | Interrupción | M | A |
| | DO8 | Factores ambientales | Destrucción de datos | Documentos expuestos al medio ambiente sin protección | Destrucción | B | M |
| | DO9 | Fallos de disponibilidad (Falta de organización de la documentación) | Ralentización y problemas en el mantenimiento del sistema | Problemas para encontrar la documentación que es precisa en un momento dado | Interrupción | M | M |
| | DO10 | Mala interpretación | Entorpecimiento de la administración y uso del sistema | Falta de claridad en la redacción de los documentos | Interrupción | B | M |
| | DO11 | Malas condiciones de conservación | Pérdida de información | Las medidas de conservación y preservación de la documentación no son las adecuadas | Pérdida | M | M |
| | DO12 | Mantenimiento inadecuado o ausente (falta de actualización) | Documentación incorrecta, redundante y compleja | No se tiene actualizada la documentación | Interrupción | M | A |
| | DO13 | Medios de datos no están disponibles cuando son necesarios | Entorpecimiento de la administración y uso del sistema | Documentación no esta de fácil acceso al personal encargado | Interrupción | B | M |
| | DO14 | Robo | Divulgación de información | La documentación ha sido sustraída | Develación | B | M |
| | DO15 | Uso sin autorización | Divulgación, robo o modificación de Información | Exposición de documentación confidencial | Develación | B | M |
| | DO16 | Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Documentación almacenada en formato digital en un medio con alta probabilidad de acción de códigos maliciosos | Destrucción | M | A |

| ACTIVO | | | | | CLASE DE AMENAZA | PROBAB. DE OCURRENCIA | IMPACTO |
|---|---|---|---|---|---|---|---|
| DATOS DEL USUARIO | COD | FACTORES DE RIESGO | CONSECUENCIA | DESCRIPCIÓN | | | |
| | DU1 | Falta de espacio de almacenamiento | Retraso de las actividades | El espacio de que disponen los usuarios para su trabajo cotidiano es insuficiente | Interrupción | B | M |
| | DU2 | Mala configuración de la programación de las copias de respaldo | Pérdida de datos del usuario | Realizar copias durante las horas en producción | Interrupción | B | B |
| | DU3 | Mala gestión de recursos compartidos | Revelación, pérdida o modificación de información | La gestión de la compartición de datos por parte de los usuarios no es la adecuada | Develación | B | M |
| | DU4 | Medios de datos no están disponibles cuando son necesarios | Retraso en las actividades | Medios de almacenamiento caros o de difícil adquisición | Interrupción | B | B |
| | DU5 | Pérdida de copias de respaldo | Pérdida de datos del usuario y retraso de la tarea | Pérdida del medio de almacenamiento o deterioro de ella | Pérdida | B | M |
| | DU6 | Perdida de confidencialidad en datos privados y de sistema | Divulgación de información | Un usuario accede a datos a los que no está autorizado | Develación | B | M |
| | DU7 | Portapapeles, impresoras o directorios compartidos | Divulgación de información | Bajo nivel de seguridad en los recursos compartidos | Develación | M | A |
| | DU8 | Robo | Divulgación de información. | Sustracción de los datos de un usuario | Develación | B | A |
| | DU9 | Sabotaje | Pérdida, modificación o divulgación de datos | Acción maliciosa sobre la información de los usuarios | Develación | B | A |
| | DU10 | Spoofing y sniffing | Divulgación, modificación y robo de información | Un intruso accede a los datos de un usuario | Develación | B | M |
| | DU11 | Virus | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Un virus se introduce en el equipo del usuario, afectando a los datos que contiene | Destrucción | M | A |

## 4.3 Análisis e Interpretación de Resultados

### 4.3.1 Valoración del Riesgo Inherente

Donde se contrasta el impacto de un riesgo junto con la probabilidad de que ocurra para ver qué riesgos han de ser tratados con mayor urgencia. Los riesgos se consignan por medio de su código asociado.

| | | PROBABILIDAD DE OCURRENCIA | | |
|---|---|---|---|---|
| | | **BAJA** | **MEDIA** | **ALTA** |
| **IMPACTO** | **BAJO** | ***BD2, EC7, EC12, CB5, CF2, CF8, AT1, IN8, DU2, DU4*** | ***SC1, CB1, CB16, US7, HD5*** | ***AT6*** |
| | **MEDIO** | ***BD6, BD12, BD14, SE8, SE9, SC2, SC5, SC7, CT4, CR1, CR2, CR3, CR7, EC3, EC6, EC9, CB6, CB7, CB8, CB10, CB12, CB13, CF4, CF5, CF13, CF14, ER1, ER6, ER9, ER11, US4, HD1, HD2, HD7, IN2, IN3, IN6, DO1, DO5, DO6, DO8, DO10, DO13, DO14, DO15, DU1, DU3, DU5, DU6, DU10*** | ***BD7, BD18, SE1, CR4, EC11, CB3, CB4, CB11, CF9, ER2, ER13, AT7, US5, US6, US8, HD3, IN7, DO4, DO9, DO11*** | ***EC17, CF3, AT5, US9, US11*** |
| | **ALTO** | ***BD1, BD3, BD5, BD8, BD9, BD10, BD16, SE2, SE3, SE5, SE6, SE10, SE12, SC8, SC10, SA1, SA2, SA3, SA4 ,SA5, SA6, SA7, SA10, CT1, CT2, CT6, CT7, CT9, CR5, CR6, CR8, CR9, CR10, EC4, EC5, EC13, EC15, EQ1, EQ2, EQ4, EQ5, CB9, CB15, CB17, CB18, CB19, CF1, CF7, CF10, CF11, ER3, ER4, ER7, ER8, ER10, ER12, AT3, AT4, AT8, AT9, US1, US14, US15, US16, US18, HD4, HD6, IN1, DO3, DU8, DU9*** | ***BD4, BD11, BD13, BD19, SE4, SE7, SC3, SC4, SC6, SC9, SA8, CT3, CT5, CT8, EC1, EC8, EC10, EC14, EC16, CB14, CF6, CF12, CF15, ER5, ER14, AT2, US2, US3, US10, US12, US13, US17, IN4, IN5, DO7, DO12, DO16, DU7, DU11*** | ***BD15, BD17, SE11, EC2, EQ3, CB2*** |

**Tabla Nº 5 – Evaluación del Impacto en la Institución**

De acuerdo al análisis realizado, se presentan las debilidades de importancia más crítica ubicadas en las celdas de color rojo y naranja de la tabla de valoración del riesgo inherente.

**Riesgo Inaceptable**

La probabilidad de ocurrencia alta e impacto alto es inaceptable porque implica la pérdida de información, de servicio y/o de recurso informático en un grado de severidad alta causando cuantiosas pérdidas.

Según el análisis estos riegos están referidos a los activos de Base de Datos (Sabotaje), Servidores (ataque por spoofing y sniffing), Equipos de Comunicación (ancho de banda insuficiente), Equipos de Seguridad (complejidad de las configuraciones) y Cableado de Fibra Óptica y Par Trenzado (ancho de banda insuficiente).

**Implementar Controles**

Esto corresponde a los sectores: probabilidad de ocurrencia media e impacto medio, probabilidad de ocurrencia media e impacto alto y probabilidad de ocurrencia alta e impacto medio.

Estos riesgos deben ser minimizados implementando controles o salvaguardas. Si es necesario atomizar el riesgo para su monitorización ya que estos deben asumirse por su probabilidad de ocurrencia. El impacto en el negocio es moderado a grave implicando con eso la perdida de información, servicios y/o recursos informáticos.

Según el análisis estos riegos están referidos a los activos de Base de Datos (transferencia de datos incorrectos), Servidores (acceso no autorizado a datos), Sistema de Correo (mal uso del servicio de correo),

Sistema de almacenamiento (falta de mantenimiento), Central de Telefonía IP y Teléfonos IP (mantenimiento inadecuado), Copias de Respaldo (copias no autorizadas), Equipos de Comunicación (abuso de puertos para el mantenimiento remoto), Cableado de Fibra Óptica y Par Trenzado (complejidad en el diseño de las redes de sistemas de TI), Código Fuente de las Aplicaciones (errores en las funciones de encriptación), Equipo de Respaldo (falta de espacio de almacenamiento), Administrador de TI (falta de auditorias), Usuarios (entrenamiento inadecuado), Hardware (errores de funcionamiento), Insumos (malas condiciones de conservación), Documentación (virus, gusanos y caballos de troya) y Datos del Usuario (portapapeles, impresoras o directorios compartidos).

**Evaluar la Necesidad de Controles**

Probabilidad de ocurrencia baja e impacto medio y alto, y probabilidad de impacto bajo y ocurrencia media y alta. Para este grupo de riesgos se tiene que evaluar el costo de la implementación de los controles versus el costo que origina la ocurrencia del riesgo. Si el costo de la ocurrencia del riesgo es mayor se deberá implementar la salvaguarda requerida. En caso contrario, se tendrá que considerar como un riesgo aceptable pero bajo medidas de monitorización para minimizar la probabilidad de ocurrencia.

Según el análisis estos riegos están referidos a los activos de Base de Datos (acceso no autorizado), Servidores (error de configuración y

operación), Sistema de Correo (virus, gusanos y caballos de troya), Sistema de Almacenamiento (administración impropia del sistema), Central de Telefonía IP y Teléfonos IP (interferencia), Copias de Respaldo (falla en medios externos), Equipos de Comunicación (corte de fluido eléctrico), Equipos de Seguridad (modificación de paquetes), Cableado de Fibra Óptica y Par Trenzado (reducción de la velocidad de transmisión), Código Fuente de las Aplicaciones (conocimiento insuficiente), Equipo de Respaldo (mala integridad de los datos resguardados), Administrador de TI (uso de derechos sin autorización), Usuarios (uso descontrolado de recursos), Hardware (robo), Insumos (limite de vida útil), Documentación (destrucción negligente de datos) y Datos del Usuario (mala gestión de recursos compartidos).

**Riesgo Aceptable**

Probabilidad de ocurrencia baja e impacto bajo, este estado es la posición de seguridad más deseada. En este entorno, las amenazas están identificadas y las salvaguardas apropiadas están en su lugar para reducir los riesgos asociados a un nivel, el cual sea aceptable para la administración de la organización.

Según el análisis estos riegos están referidos a los activos de Base de Datos (base de datos compleja), Equipos de Comunicación (falta de autenticación), Cableado de Fibra Óptica y Par Trenzado (conexión de cables inadmisible), Código Fuente de las Aplicaciones (falta de compatibilidad), Administrador de TI (administración impropia del

sistema de TI), Insumos (transporte inseguro) y Datos del Usuario (medios de datos no disponibles cuando son necesarios).

### 4.3.2 Elección de Salvaguardas

Al tener identificados los riesgos, junto con las probabilidades de ocurrencia e impacto que podrían causar, se puede realizar una evaluación y priorización de los riesgos y definir el nivel de aceptación de riesgo que la organización esta dispuesta a aceptar.

A continuación, se detallan los controles definidos para cada uno de los riesgos identificados con el fin de minimizar el impacto que pudiera tener su ocurrencia en la organización.

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| BASE DE DATOS | BD1 | Acceso no autorizado a datos (borrado, modificación, etc.) | Pérdida, revelación o modificación de datos; pérdida de tiempo y productividad | Seguridad física y control de acceso lógico |
| | BD2 | Base de datos compleja | Desarrollo complejo de sistemas | Definir estructuras simples de ser posibles y documentarlas |
| | BD3 | Copia no autorizada de un medio de datos | Divulgación de información | Deshabilitación del portapapeles y controles lógicos |
| | BD4 | Errores de software | Inconsistencia en los datos | Controles internos y copias de respaldo de los datos |
| | BD5 | Falla de base de datos | Inconsistencia en los datos | Controles internos y backup de los datos |
| | BD6 | Falta de espacio de almacenamiento | Falla en la aplicación | Recursos abundantes |
| | BD7 | Mala configuración de la programación de las copias de respaldo | Datos sin backup | Organización de la programación |
| | BD8 | Mala integridad de los datos | Inconsistencia y redundancia de datos | Controles en las aplicaciones desarrolladas |
| | BD9 | Medios de datos no están disponibles cuando son necesarios | Pérdida de tiempo y productividad | Mantenimiento regular del sistema |
| | BD10 | Pérdida de copias de respaldo | Incapacidad de restauración | Copias de respaldo redundantes |
| | BD11 | Perdida de confidencialidad en datos privados y de sistema | Divulgación de información | Controles físicos y controles de accesos lógicos a datos críticos |
| | BD12 | Perdida de datos en tránsito | Inconsistencia de datos y divulgación de información | Políticas de configuración de red |
| | BD13 | Portapapeles, impresoras o directorios compartidos | Divulgación de información | Deshabilitación del portapapeles y controles lógicos |
| | BD14 | Robo | Pérdida de información | Deshabilitación del portapapeles y controles lógicos |
| | BD15 | Sabotaje | Pérdida o modificación de datos, pérdida de tiempo y productividad | Copias de respaldo redundantes y controles físicos y lógicos |
| | BD16 | Seguridad de base de datos deficiente | Perdida o modificación de datos | Políticas de seguridad de información |
| | BD17 | Spoofing y sniffing | Divulgación y modificación de información | Copias de respaldo redundantes y controles físicos y lógicos |
| | BD18 | Transferencia de datos incorrectos | Inconsistencia de datos | Controles lógicos |
| | BD19 | Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Herramientas antivirus y firewall |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| SERVIDORES | SE1 | Acceso no autorizado a datos | Robo, modificación de información | Seguridad física y control de acceso lógico |
| | SE2 | Acceso no autorizado a equipos | Robo, modificación de información | Seguridad física y control de acceso lógico |
| | SE3 | Corte de luz, UPS descargado o variaciones de voltaje | Falta de sistema | Generador, UPS, estabilizador, tres líneas independientes |
| | SE4 | Destrucción o mal funcionamiento de un componente | Pérdida de tiempo por necesidad de reemplazo | Redundancia de los componentes del servidor. |
| | SE5 | Error de configuración y operación | Aumento de vulnerabilidades e inestabilidad en el sistema | Contratación de mantenimiento por especialistas |
| | SE6 | Factores ambientales | Falta de sistema y destrucción de equipos | Seguridad física y buen diseño del edificio |
| | SE7 | Límite de vida útil - Máquinas obsoletas | Deterioro en la performance del sistema | Equipamiento actual y asesoramiento permanente |
| | SE8 | Mal mantenimiento | Interrupciones en el funcionamiento del sistema | Mantenimiento interno en manos de especialistas |
| | SE9 | Modificación no autorizada de datos | Inconsistencia de datos, mala configuración, fraude | Controles de acceso físico y lógico al servidor |
| | SE10 | Robo | Pérdida de equipamiento o información | Controles de acceso físicos, guardias de seguridad, alarmas |
| | SE11 | Spoofing y sniffing | Divulgación, modificación y robo de información | Monitorización permanente de la red |
| | SE12 | Virus, gusanos y caballos de Troya | Fallas generales del sistema y en la red | Herramientas antivirus y firewall |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| SISTEMA DE CORREO | SC1 | Cuentas de correo activas de ex - usuarios | Uso indebido del servicio | Coordinación con la el Sistema Único de Matrícula |
| | SC2 | Errores en las funciones de encriptación | Divulgación de información (contraseñas) | Personal de operación especializado |
| | SC3 | Falta de autenticación | Exposición de información | Controles de acceso a datos y a equipos estrictos |
| | SC4 | Mal uso del servicio de correo | Disminución de la performance del ancho de banda | Concienciación de los usuarios sobre el buen uso del correo |
| | SC5 | Mala integridad de los datos | Inconsistencia de información | Resguardo de la Información |
| | SC6 | Perdida de confidencialidad en datos privados y de sistema | Divulgación de información | Controles físicos y controles de accesos lógicos a datos críticos |
| | SC7 | Perdida de datos en tránsito | Pérdida de información | Políticas de configuración de red |
| | SC8 | Sabotaje | Pérdida del servicio | Copias de respaldo redundantes y controles físicos y lógicos |
| | SC9 | Spoofing y sniffing | Divulgación, modificación y robo de información | Copias de respaldo redundantes y controles físicos y lógicos |
| | SC10 | Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Herramientas antivirus y firewall |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| SISTEMA DE ALMACENAMIENTO(SAN) | SA1 | Acceso no autorizado a equipos | Robo, modificación de información | Seguridad física y control de acceso lógico |
| | SA2 | Administración impropia del sistema | Modificación de datos, perdida de la configuración | Administración por personal profesional |
| | SA3 | Condiciones de trabajo adversas | Pérdida de datos, deterioro del equipo | Ambiente de trabajo cómodo |
| | SA4 | Daño de cables inadvertido | Pérdida e interrupción de datos | Seguridad física |
| | SA5 | Falla en la SAN | Pérdida de información, paralización del servicio | Seguridad física y copias de respaldo |
| | SA6 | Falla en medios externos | Pérdida de datos en medios externos | Redundancia de medios externos |
| | SA7 | Mala integridad de los datos | Inconsistencia de información | Copias de respaldo |
| | SA8 | Mantenimiento inadecuado o ausente | Perdida o deterioro de datos | El mantenimiento diario lo realiza el administrador de sistemas, ayudado por un especialista contratado |
| | SA9 | Medios de datos no están disponibles cuando son necesarios | Pérdida de tiempo y productividad por falta de datos | Mantenimiento regular del sistema |
| | SA10 | Sabotaje | Pérdida o robo de información | Copias de respaldo redundantes y controles físicos y lógicos |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| CENTRAL DE TELEFÓNICA IP Y TELÉFONOS IP | CT1 | Acceso no autorizado a equipos | Robo, modificación de información | Seguridad física y control de acceso lógico |
| | CT2 | Administración impropia del sistema | Modificación de datos, perdida de la configuración | Administración por personal profesional |
| | CT3 | Ancho de banda insuficiente | Interrupción del servicio | Recursos abundantes en ancho de banda |
| | CT4 | Conexiones de cables inadmisible | Interrupción del servicio | Cableado estructurado aplicado en el tendido de la empresa |
| | CT5 | Conservación deficiente | Interrupción del servicio | Adecuado ambiente de conservación |
| | CT6 | Factores ambientales | Interrupción del servicio | Utilización de UPS y buen diseño del edificio |
| | CT7 | Interferencia | Perdida del servicio | Mantenimiento de sistema radial |
| | CT8 | Mantenimiento inadecuado o ausente | Perdida o deterioro de equipos | Mantenimiento por especialistas |
| | CT9 | Sabotaje | Interrupción del servicio | Controles de acceso físicos, guardias de seguridad |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| COPIAS DE RESPLADO | CR1 | Accesos no autorizados al medio de almacenamiento | Perdida, alteración o revelación de información | Seguridad física y control de acceso lógico |
| | CR2 | Clasificación deficiente de medios | Pérdida de medios de almacenamiento o retrasos en su restauración | Rotulamiento y orden de clasificación |
| | CR3 | Conservación deficiente | Problemas en la restauración de la información | Adecuado ambiente de conservación |
| | CR4 | Copia no autorizada de un medio de datos | Robo de información | Controles de seguridad física en el ingreso al centro de cómputos y controles de acceso lógicos al servidor |
| | CR5 | Errores de respaldo | Problemas en la restauración de información | Numerosas copias de respaldo por posibles errores |
| | CR6 | Falla en medios externos | Pérdida de datos en medios externos | Copias redundantes en distintos medios de almacenamiento |
| | CR7 | Fallos en la disponibilidad de medios | Pérdida de medios de almacenamiento o retrasos en su restauración | Numerosas copias de respaldo por posibles errores |
| | CR8 | Pérdida de medios | Imposibilidad de restauración de información | Backups redundantes |
| | CR9 | Robo | Pérdida de información, imposibilidad de restauración | Controles de acceso físicos, guardias de seguridad, alarmas |
| | CR10 | Sabotaje | Pérdida o robo de información | Controles de acceso físicos, guardias de seguridad y copias de respaldo redundantes |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| EQUIPOS DE COMUNICACIÓN (ROUTERS, SWITCHES, HUBS, ETC.) | EC1 | Abuso de puertos para el mantenimiento remoto | Posibles intrusiones y robo o divulgación de información | Política de configuración de puertos restringida y herramientas de monitoreo de puertos |
| | EC2 | Ancho de banda insuficiente | Ralentización de la transmisión de información | Recursos abundantes en ancho de banda |
| | EC3 | Configuración inadecuada de componentes de red | Errores de transmisión, interrupción del servicio de red | Equipamiento de red configurado por personal profesional |
| | EC4 | Corte de luz, UPS descargado o variaciones de voltaje | Interrupción de las transmisiones | Generador, UPS, estabilizador, tres líneas independientes |
| | EC5 | Denegación de servicio | Interrupción de todos o algunos de los servicios de red | Firewall y políticas de seguridad |
| | EC6 | Errores de operación | Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades | El mantenimiento diario lo realiza el administrador de sistemas, ayudado por un especialista contratado |
| | EC7 | Falta de autenticación | Posibles intrusiones y robo o divulgación de información | Controles de acceso a datos y a equipos, y firewall |
| | EC8 | Límite de vida útil - Máquinas obsoletas | Uso deficiente del sistema | equipamiento actuales, de respaldo y asegurado |
| | EC9 | Mantenimiento deficiente | Errores de transmisión, mal funcionamiento de la red | El mantenimiento diario lo realiza el administrador de sistemas, ayudado por un especialista contratado |
| | EC10 | Modificación de paquetes | Alteración de la información | Políticas de seguridad, Controles físicos y lógicos |
| | EC11 | Penetración, intercepción o manipulación del medio de transporte | Robo de información | Controles físicos y lógicos |
| | EC12 | Perdida de datos en tránsito | Divulgación de información | Controles físicos y lógicos |
| | EC13 | Robo | Interrupción de la transmisión, gastos de reposición | Controles de acceso físicos, guardias de seguridad, alarmas |
| | EC14 | Sabotaje | Red inaccesible | Controles físicos y lógicos |
| | EC15 | Sincronización de tiempo inadecuada | Inconsistencia en datos | Aplicativo que actualiza el horario permanentemente. |
| | EC16 | Spoofing y sniffing | Divulgación, modificación y robo de información | Copias de respaldo redundantes y controles físicos y lógicos |
| | EC17 | Velocidad de transmisión insuficiente | Ralentización de la transmisión de información | Recursos abundantes en ancho de banda |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| EQUIPOS DE SEGURIDAD | EQ1 | Acceso no autorizado a equipos | Robo, modificación de información | Seguridad física y control de acceso lógico |
| | EQ2 | Administración impropia del sistema | Modificación de datos, perdida de la configuración | Administración por personal profesional |
| | EQ3 | Complejidad de las configuraciones | Administración mas laboriosa | Analizar y sumarizar sentencias para reducir la cantidad de datos a ingresar |
| | EQ4 | Modificación de paquetes | Alteración de la información | Políticas de seguridad, Controles físicos y lógicos |
| | EQ5 | Sabotaje | Pérdida o robo de información | Controles físicos y lógicos |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| CABLEADO DE FIBRA ÓPTICA Y PAR TRENZADO (UTP) | CB1 | Abuso de puertos para el mantenimiento remoto | Posibles intrusiones y robo o divulgación de información | Política de configuración de puertos restringida y herramientas de monitoreo de puertos |
| | CB2 | Ancho de banda insuficiente | Transmisión pesada en la red o imposibilidad de utilizar el sistema en línea | Recursos abundantes en ancho de banda |
| | CB3 | Ausencia o falta de segmentación | Tramos de red extensos y dificultades en la comunicación | Red segmentada física y lógicamente por sectores |
| | CB4 | Complejidad en el diseño de las redes de sistemas de TI | Dificultad en la administración y en el mantenimiento | Diseño de red simple con topología de bus |
| | CB5 | Conexión de cables inadmisible | Robo de datos, spoofing y sniffing | Cableado estructurado aplicado en el tendido de la empresa |
| | CB6 | Conexiones todavía activas | Intrusión de usuarios no autorizados al sistema | Auditoria de cableado estructurado |
| | CB7 | Daño o destrucción de cables o equipamiento inadvertido | Pinchaduras de cables, robo de datos, spoofing y sniffing | Cableado estructurado aplicado en el tendido de la empresa |
| | CB8 | Factores ambientales | Interferencias o daños de equipamiento | Utilización de UPS y buen diseño del edificio |
| | CB9 | Falla en la SAN | Una o más servidores incomunicados | Mantenimiento por especialistas sobre SAN |
| | CB10 | Interferencias | Errores en los datos de transmisión o imposibilidad de utilizar los servicios en línea | Cableado estructurado en la red de la Universidad y mantenimiento de sistema radial |
| | CB11 | Límite de vida útil del cableado estructurado | Cableado obsoleto y deterioro de la comunicación | Equipamiento actualizado y mantenimiento del cableado |
| | CB12 | Longitud de los cables de red excedida | Transmisión lenta o con interferencias, o imposibilidad de utilizar los servicios de red | Cableado estructurado y mantenimiento del cableado |
| | CB13 | Mal mantenimiento | Errores de transmisión o interrupción del servicio de red | Mantenimiento por especialistas en cableado estructurado |
| | CB14 | Penetración, intercepción o manipulación del medio de transporte | Robo de información | Controles físicos y lógicos |
| | CB15 | Perdida de datos en tránsito | Divulgación de información | Controles físicos y lógicos |
| | CB16 | Reducción de velocidad de transmisión | Pérdida de tiempo de los usuarios, o imposibilidad de utilizar los servicios de red | Recursos abundantes en ancho de banda, políticas de uso de recursos |
| | CB17 | Riesgo por el personal de limpieza o personal externo | Daño en cables o equipos, interrupción del servicio | Cables y equipos protegidos, fuera de la vista y el alcance de terceros |
| | CB18 | Sabotaje | Pérdida o robo de información | Controles físicos y lógicos |
| | CB19 | Transporte inseguro de archivos | Divulgación de información | Controles lógicos |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| CÓDIGO FUENTE DE LAS APLICACIONES | CF1 | Acceso no autorizado a datos (borrado, modificación, etc.) | Modificación del software en desarrollo | Controles físicos y controles de accesos lógicos a desarrollo de software |
| | CF2 | Aplicaciones obsoletas | Disminución de productividad, mayor sensibilidad a vulnerabilidades | Renovación de aplicaciones |
| | CF3 | Aplicaciones sin licencia | Multas y problemas con Software Legal | Licenciamiento de los productos a utilizar |
| | CF4 | Conocimiento insuficiente de los documentos de requerimientos en el desarrollo | Sistema inestable y excesivo pedido de cambios | Metodología de análisis y diseño estructurada |
| | CF5 | Error de configuración y operación | Mal funcionamiento de los sistemas | Existen herramientas de análisis y personal de mantenimiento |
| | CF6 | Errores en las funciones de encriptación | Problemas en la recuperación de archivos encriptados o divulgación de información | Personal de mantenimiento especializado |
| | CF7 | Falla del sistema | Falta de sistema y posibles demoras | Copias de respaldo y sistemas de respaldo |
| | CF8 | Falta de compatibilidad | Datos erróneos e inestabilidad del sistema | Herramienta de comunicación entre sistemas operativos diferentes |
| | CF9 | Falta de confidencialidad | Divulgación de información | Deshabilitación del portapapeles y controles lógicos |
| | CF10 | Mala administración de control de acceso (salteo del login, etc.) | Divulgación y modificación de información | Controles de acceso lógico, reforzados en datos críticos |
| | CF11 | Pérdida de código fuente | Divulgación de información | Copias de respaldo |
| | CF12 | Poca adaptación a cambios del sistema | Sistema inestable y de difícil modificación | Metodología de análisis y diseño estructurada |
| | CF13 | Prueba de software deficiente | Sistema poco confiable | Metodología de análisis y diseño estructurada |
| | CF14 | Software desactualizado | Probabilidad incremental de vulnerabilidades y virus | Mantenimiento por especialistas y constante evaluación de las aplicaciones |
| | CF15 | Virus, gusanos y caballos de Troya | Inestabilidad y mal funcionamiento de sistemas | Herramientas antivirus y firewall |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| EQUIPO DE RESPALDO (BACKUPS) | ER1 | Conservación deficiente | Pérdida de información, imposibilidad de restauración | Ambiente adecuado para el equipo de respaldo |
| | ER2 | Copia no autorizada a un medio de datos | Robo de información | Controles de seguridad física, controles de acceso lógicos a los sistemas |
| | ER3 | Errores de software | Error en la generación o en la copia de respaldo a medios externos | Controles internos y copias de respaldo de los datos |
| | ER4 | Falla en medios externos | Pérdida de copias de respaldo | Copias de respaldo redundantes en distintos medios de almacenamiento |
| | ER5 | Falta de espacio de almacenamiento | Falla en la generación de copias de respaldo | Existencia de discos redundantes para la copia |
| | ER6 | Mala configuración de la programación de las copias de respaldo | Falta de copias de respaldo de datos | Agenda de programación eficiente |
| | ER7 | Mala integridad de los datos resguardados | Errores durante la restauración de datos | Numerosas copias de respaldo por posibles errores |
| | ER8 | Medios de datos no están disponibles cuando son necesarios | Pérdida de copias de respaldo y retraso del sistema | Numerosas copias de respaldo por posibles errores |
| | ER9 | Pérdida de copias de respaldo | Falta de datos, incapacidad de restaurarlos y divulgación de información | Copias de respaldo redundantes |
| | ER10 | Robo | Incapacidad de restaurarlos y divulgación de información | Controles de acceso físicos, guardias de seguridad, alarmas |
| | ER11 | Rótulos inadecuado en los medios de datos | Errores durante la restauración de datos | Rótulos capaces de diferenciar cada medio de datos como único |
| | ER12 | Sabotaje | Pérdida o robo de información | Controles de acceso físicos, guardias de seguridad y copias de respaldo redundantes |
| | ER13 | Spoofing y sniffing | Divulgación, modificación y robo de información | Monitorización de la red |
| | ER14 | Virus, gusanos y caballos de Troya | Pérdida de datos de copias de respaldo | Herramientas antivirus y firewall |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| ADMINISTRADOR DE TI | AT1 | Administración impropia del sistema de IT (responsabilidades y roles del personal de sistemas) | Asignación de responsabilidades impropia | Administración por personal profesional |
| | AT2 | Almacenamiento de contraseñas negligente | Divulgación de contraseñas y uso indebido de derechos de usuarios | El sistema operativo encripta las contraseñas de sus usuarios, y se ha modificado el directorio de almacenamiento por defecto |
| | AT3 | Configuración impropia del Postfix | Divulgación de mensajes, uso del servidor para enviar SPAM, fallas en la administración de cuotas de discos | La configuración del Postfix la realiza y mantiene un especialista en la aplicación |
| | AT4 | Errores de configuración y operación del sistema | Inestabilidad del sistema, reducción de la performance y aumento de las vulnerabilidades | El mantenimiento diario lo realiza el administrador de sistemas, ayudado por un especialista contratado. |
| | AT5 | Falta de auditorías en sistemas informáticos | Imposibilidad del seguimiento de usuarios y de la generación de reportes | Existen logs generados automáticamente por los sistemas y por sus aplicaciones principales |
| | AT6 | Mala evaluación de datos de auditoría | No se analizan los logs y por lo tanto no hay evaluación de los resultados | Trabajo debe ser realizado por personal profesional |
| | AT7 | Mal uso de derechos de administrador | Mala distribución de los permisos y de las cuentas de administrador | Administración por personal calificado |
| | AT8 | Uso de derechos sin autorización | Robo de información | Políticas de Administración y seguridad |
| | AT9 | Uso impropio del sistema de IT | Administración deficiente | Administración y operación por personal profesional |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| USUARIOS | US1 | Acceso no autorizado a datos | Divulgación o robo de información | Controles de acceso lógico a datos en las aplicaciones |
| | US2 | Borrado, modificación o revelación desautorizada o inadvertida de información | Inconsistencia de datos o datos faltantes | Controles lógicos a datos |
| | US3 | Condiciones de trabajo adversas | Predisposición a distracción, bajo rendimiento de usuarios | Ambiente de trabajo cómodo |
| | US4 | Destrucción de un componente de hardware | Pérdida de tiempo por necesidad de reemplazo | Redundancia de los componentes |
| | US5 | Destrucción negligente de datos | Pérdida de información | Controles lógicos a datos en las aplicaciones. |
| | US6 | Desvinculación del personal | Robo o modificación de información, sabotaje interno | Establecer procedimiento formal de desvinculación |
| | US7 | Documentación deficiente | Mayor probabilidad de errores por falta de instrucciones | Mantener actualizado la documentación necesaria de función y operación |
| | US8 | Entrada sin autorización a los ambientes | Robo de equipos o insumos, divulgación de datos | Control de acceso físico a instalaciones del centro de cómputos |
| | US9 | Entrenamiento de usuarios inadecuado | Predisposición a errores y bajo rendimiento de usuarios | Capacitación grupal de usuarios en el uso del sistema |
| | US10 | Errores en el control de permisos y privilegios | Robo de información | Auditorías en el control lógico |
| | US11 | Falta de auditorías | Predisposición a un rendimiento mediocre y falta de concienciación sobre responsabilidades y seguridad | Implementar estándar de auditoria informática |
| | US12 | Falta de cuidado en el manejo de la información (Ej. Contraseña) | Divulgación de datos | Insistencia con respecto al uso discreto de datos críticos |
| | US13 | Ingeniería social - Ingeniería social inversa | Robo o modificación de información | Políticas, normas de seguridad y programa de concientización |
| | US14 | Mal uso de derechos de administrador (sesiones abiertas) | Divulgación o robo de información, sabotaje interno | Controles de seguridad lógica |
| | US15 | No-cumplimiento con las medidas de seguridad del sistema | Medidas correctivas tomadas por la gerencia, según la gravedad del incidente | Permanente concienciación de los usuarios |
| | US16 | Pérdida de confidencialidad o integridad de datos como resultado de un error humano | Error en la información | Controles lógicos de acceso a datos y de integridad de datos de entrada al sistema |
| | US17 | Problemas en el acceso físico a equipos | Respuesta tardía a evento | Coordinación con el personal encargado |
| | US18 | Uso descontrolado de recursos | Retraso en las actividades o falta de sistema | Administración eficiente de los recursos |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| HARDWARE | HD1 | Corte de luz, UPS descargado o variaciones de voltaje | Interrupción del funcionamiento de equipos | Generador, UPS, estabilizador, tres líneas independientes |
| | HD2 | Destrucción o mal funcionamiento de un componente | Interrupción de la tarea del usuario | Insumos de respaldo y equipamiento asegurado |
| | HD3 | Errores de funcionamiento | Interrupción/problemas en el funcionamiento del sistema | Insumos de respaldo y equipamiento asegurado |
| | HD4 | Factores ambientales | Destrucción o avería de equipos | Insumos de respaldo y equipamiento asegurado |
| | HD5 | Límite de vida útil | Avería de equipos | Insumos de respaldo y equipamiento asegurado |
| | HD6 | Mal mantenimiento | Avería de equipos e incremento en el costo de equipamiento de respaldo | El mantenimiento diario lo realiza el administrador de sistemas, ayudado por un especialista contratado |
| | HD7 | Robo | Pérdida de equipamiento e interrupción de la tarea del usuario | Controles de acceso físicos, guardias de seguridad, alarmas |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| INSUMOS | IN1 | Factores ambientales | Destrucción de insumos | Insumos de respaldo |
| | IN2 | Límite de vida útil | Destrucción o avería de los insumos | Insumos de respaldo |
| | IN3 | Mala disponibilidad | Ralentización de las actividades | Insumos de respaldo |
| | IN4 | Malas condiciones de conservación | Destrucción o avería de los insumos | Ambientes adecuados de conservación |
| | IN5 | Recursos escasos (recorte presupuestal) | Interrupción en el funcionamiento normal del sistema | Insumos de respaldo. |
| | IN6 | Uso descontrolado de recursos | Incremento no justificado del gasto de insumos | Administración estricta de insumos |
| | IN7 | Robo | Pérdida de insumos e incremento en el gasto | Controles de acceso físicos, guardias de seguridad, alarmas |
| | IN8 | Transporte inseguro de insumos | Pérdida de insumos, e incremento en el gasto | Personal asignado a dicha tarea con normas internas a cumplir |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| DOCUMENTACIÓN | DO1 | Acceso no autorizado a datos de documentación | Divulgación, robo o modificación de información | Control de acceso físico a instalaciones del centro de cómputos |
| | DO2 | Borrado o modificación desautorizada de información | Documentación incorrecta | Copia de respaldo de la información |
| | DO3 | Rebuscar información | Divulgación de información | Controles de acceso lógico al sistema |
| | DO4 | Copia no autorizada de un medio de datos | Divulgación de información | Control de acceso físico a instalaciones del centro de cómputos |
| | DO5 | Descripción de archivos inadecuada | Documentación incorrecta | Estandarización de la descripción de archivos |
| | DO6 | Destrucción negligente de datos | Documentación incorrecta | Copia de respaldo de la información |
| | DO7 | Documentación insuficiente o faltante, funciones no documentadas | Entorpecimiento de la administración y uso del sistema | Documentación estandarizada y eficiente |
| | DO8 | Factores ambientales | Destrucción de datos | Seguridad física y buen diseño del edificio |
| | DO9 | Fallos de disponibilidad (Falta de organización de la documentación) | Ralentización y problemas en el mantenimiento del sistema | Adquisición de material bibliográfico sobre el tema |
| | DO10 | Mala interpretación | Entorpecimiento de la administración y uso del sistema | Adquisición de material bibliográfico de fácil uso y comprensión |
| | DO11 | Malas condiciones de conservación | Pérdida de información | Ambientes adecuados de conservación |
| | DO12 | Mantenimiento inadecuado o ausente (falta de actualización) | Documentación incorrecta, redundante y compleja | Programación de mantenimiento y actualización |
| | DO13 | Medios de datos no están disponibles cuando son necesarios | Entorpecimiento de la administración y uso del sistema | Insumos y equipos de respaldo |
| | DO14 | Robo | Divulgación de información | Controles de acceso físico a datos |
| | DO15 | Uso sin autorización | Divulgación, robo o modificación de Información | Controles de acceso físico a datos |
| | DO16 | Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Herramientas antivirus y firewall |

| | COD | FACTORES DE RIESGO | CONSECUENCIA | SOLUCIÓN |
|---|---|---|---|---|
| DATOS DEL USUARIO | DU1 | Falta de espacio de almacenamiento | Retraso de las actividades | Capacidad de almacenamiento sobredimensionada. |
| | DU2 | Mala configuración de la programación de las copias de respaldo | Pérdida de datos del usuario | Programación realizada por personal profesional |
| | DU3 | Mala gestión de recursos compartidos | Revelación, pérdida o modificación de información | Tratar en lo mínimo de no compartir recursos, aplicar controles lógicos de seguridad |
| | DU4 | Medios de datos no están disponibles cuando son necesarios | Retraso en las actividades | Permanente disponibilidad de estos medios por personal del centro de cómputos |
| | DU5 | Pérdida de copias de respaldo | Pérdida de datos del usuario y retraso de la tarea | Controles de acceso físico y lógico al equipo usado para tal copias de respaldo |
| | DU6 | Perdida de confidencialidad en datos privados y de sistema | Divulgación de información | Controles de acceso físico y lógico a las PC´s de los usuarios |
| | DU7 | Portapapeles, impresoras o directorios compartidos | Divulgación de información | Carpetas de usuarios no compartidas en la red |
| | DU8 | Robo | Divulgación de información. | Controles de acceso físico y lógico a los equipos |
| | DU9 | Sabotaje | Pérdida, modificación o divulgación de datos | Controles de acceso físico y lógico a los equipos y copias de respaldo de los datos |
| | DU10 | Spoofing y sniffing | Divulgación, modificación y robo de información | Copias de respaldo redundantes y controles físicos y lógicos |
| | DU11 | Virus, gusanos y caballos de Troya | Pérdida, modificación o divulgación de datos, pérdida de tiempo, y productividad | Herramientas antivirus y firewall. |

# CAPÍTULO V

## 5. CONCLUSIONES

A lo largo del presente trabajo se pudo comprender que la seguridad informática es un conjunto de recursos destinados a lograr que la información y los activos de una organización sean confidenciales, íntegros y disponibles para todos sus usuarios.

De acuerdo a los resultados del Análisis de Riesgo realizado utilizando el método cualitativo, la UNMSM cuenta con salvaguardas implementadas, las que condicionan a que la mayor parte de los riesgos sean de probabilidad de ocurrencia baja. Según la tabla de Análisis de Impacto (ver Tabla Nº 5, página 108), se observa que la gran mayoría de riesgos que presenta la UNMSM son de probabilidad baja, pero no por ello dejan de ser insignificantes ya que muchos de ellos presentan un impacto alto.

Somos conscientes de que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo se debe estar preparado y dispuesto a reaccionar con rapidez ya que las amenazas y las vulnerabilidades están cambiando constantemente.

Disponer de una política de seguridad es importante, pero entendemos que hacer de la política de seguridad una parte del entorno de trabajo diario es esencial. La comunicación con los usuarios es la clave para hacer que esta política sea efectiva y se genere una “cultura de la seguridad”. La seguridad en la información no es posible sin la cooperación del usuario. Se puede tener la mejor tecnología para protegerlos y aún así, sufrir una ruptura de seguridad.

La implantación de una política de seguridad informática en una organización implica un gran desafío, pero sabemos además que es imprescindible, sobre todo si se tiene en cuenta que cada vez se produce un mayor número de ataques.

Ha de hacerse hincapié en que este trabajo se encuentra en un período de continua actualización por lo que ha de ser objeto de revisión y retroalimentación frecuentes debido a la naturaleza cambiante de las amenazas que a diario acechan a los sistemas de información.

Debe quedar claro que la Seguridad Informática es un aspecto muchas veces descuidado en nuestros sistemas, pero de vital importancia para el correcto funcionamiento de todos ellos. La Seguridad es un proceso NO un producto.

Por último, se espera con este trabajo generar en el lector una inquietud que incite a futuras investigaciones o proyectos que profundicen en el campo de la seguridad informática.

## Conclusiones Adicionales

### Aislamiento Vs Globalización

Abierta, Universal, Económica y Segura. Esas son las propiedades que adjudican algunos a la información. Lograr estándares en el mundo altamente tecnificado de hoy es quizás la principal barrera con las que chocan los profesionales para “asegurar la Seguridad”.

Por otro lado, la situación internacional actual exige una concientización, por parte de todos, que la información es conocimiento y como tal debemos atribuirle la importancia que merece. Esta importancia incluye estudiar y lograr la forma de protegerla.

Esto plantea una paradoja:

- Si sumamos seguridad, bajan las posibilidades de acceder a la información, lo que es igual al Aislamiento y la Marginación.
- Si sumamos información, lo hacemos de forma insegura, lo que nos hace Globalmente Vulnerables.

La convergencia de los sistemas multiplica exponencialmente los problemas de seguridad planteados. El equilibro es difícil, el espectro a cubrir es amplio y, como dificultad extra, el campo de trabajo es intangible. Esto hace necesario desarrollar técnicas y/o adaptar las existentes de forma tal de circunscribir nuestro trabajo de conseguir información–conocimiento dentro de un marco de seguridad.

**Diseño Seguro Requerido**

Cuando se diseña un sistema se lo hace pensando en su Operatividad–Funcionalidad dejando de lado la Seguridad.

Será necesario establecer una correspondencia y pertenencia entre las técnicas adoptadas conformando un sistema de seguridad; y no procedimientos aislados que contribuyan al caos general existente. Esto sólo puede lograrse al integrar la seguridad desde el comienzo, desde el diseño, desde el desarrollo.

**Tecnología Existente**

Existen infinidad de métodos (muchas veces plasmados en herramientas) que permiten violar un sistema.

El profesional cuenta con la misma tecnología para la evaluación de la seguridad del bien a proteger y otras pensadas para la protección como fin. Esto hace que muchas veces, la seguridad, sea asunto de la idoneidad del profesional.

En algunos campos, la Tecnología deberá ampararnos ante la desaparición de elementos naturales. Por mencionar un ejemplo: la firma digital (Tecnología Criptográfíca) debe cubrir la brecha que deja la inexistencia de la firma caligráfica en archivos de información.

**Daños Minimizables**

Algunos pocos métodos realmente novedosos de infiltración ponen en jaque los sistemas de seguridad. Aquí, se prueba la incapacidad de lograr 100% de

seguridad, pero también es hora de probar que los riesgos, la amenaza, y por ende los daños pueden ser llevados a su mínima expresión.

Muchas veces basta con restringir accesos a información no utilizada o que no corresponde a los fines planteados. Otras veces la capacitación será la mejor herramienta para disminuir drásticamente los daños.

**Riesgos Manejables**

Se ha probado que: La Seguridad Perfecta requiere un nivel de perfección que realmente no existe, y de hecho se duda que algún día existirá, pero los riesgos deben y pueden ser manejables.

**Costos**

El costo en el que se incurre suele ser una fruslería comparados con aquellos luego de producido un daño. El desconocimiento y la falta de información son el principal inconveniente cuando se evalúa la inclusión de seguridad como parte de un sistema.

**Personas Involucradas**

Es una realidad que la Seguridad involucra manipulación de naturaleza humana.

Es importante comprender que:

1. La Seguridad consiste en Tecnología y Política. Es decir que la combinación de la Tecnología y su forma de utilización determina cuan seguros son los sistemas.

2. El problema de la Seguridad no puede ser resuelto por única vez. Es decir que constituye un viaje permanente y no un destino.

3. En última instancia la Seguridad es una serie de movimientos entre “buenos” y “malos”.

# CAPÍTULO VI

## 6. RECOMENDACIONES

Dentro de las principales recomendaciones tenemos:

- La clave para desarrollar con éxito un programa efectivo de seguridad de la información consiste en recordar que las políticas, estándares y procedimientos de seguridad de la información son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica. Muchas organizaciones ignoran esta interrelación en un esfuerzo por simplificar el proceso de desarrollo. Sin embargo, estas mismas relaciones son las que permiten que las organizaciones exijan y cumplan los requerimientos de seguridad. Pero para dar inicio a un plan, política o procedimiento de seguridad es necesario realizar previamente un “Análisis de Riesgo”.

- Por lo general se argumenta que las organizaciones requieren una Política de Seguridad de la Información para cumplir con sus "requerimientos de seguridad de la información". Sin embargo, una política de seguridad no puede ser elaborada sin tener conocimiento de los activos (hardware, software y datos) que se quieren proteger y los riesgos a los que están

expuestos estos activos. Para ello es imprescindible la elaboración de un Análisis de Riesgo inicial y luego la administración de ella para mantener la continuidad de detección de nuevas amenazas.

- La Administración de Riesgos es un ciclo evolutivo que comprende: análisis y evaluación de riesgo, implementación de salvaguardas, monitorización de los riesgos y mantenimiento y mejora de los controles. Para mitigar la probabilidad de ocurrencia de un riesgo es necesario la implementación de una Política de Seguridad de la Información, ya que ésta exige que todos en la organización protejan la información para que la empresa pueda cumplir con sus responsabilidades reglamentarias, jurídicas y fiduciarias. Se usa mal y con frecuencia las palabras "generalmente" y "proteger" para justificar mayor inversión cuando no es necesaria. Esto puede parecer contrario a la intuición, pero la inversión adicional para proteger la información no siempre garantiza el éxito. Pero si es recomendable tener un presupuesto asignado para cumplir con estos fines. Para evaluar las necesidades de inversión, debe consultar estas "reglas" en orden secuencial:

  **Regla Nº 1:** Saber qué información tiene y donde se encuentra. (Valoración de activos)

  **Regla Nº 2:** Saber el valor de la información que se tiene y la dificultad de volverla a crear si se daña o pierde. (Evaluación y análisis de riesgos)

  **Regla Nº 3:** Saber quiénes están autorizados para acceder a la información y que pueden hacer con ella. (Políticas de seguridad)

**Regla Nº 4:** Saber la velocidad con que puede acceder a la información si no está disponible por alguna razón (por pérdida, modificación no autorizada, etc.)

Estas cuatro reglas son aparentemente simples. Sin embargo, las respuestas permitirán el diseño e implementación de un programa de protección a la información puesto que las respuestas pueden ser muy difíciles. No toda la información tiene el mismo valor y por lo tanto no requiere el mismo nivel de protección (con el costo que implica).

- **Es clave entender por qué se necesita proteger la información,** desde un punto de vista comercial es clave determinar la necesidad de tener una Política de Seguridad de la Información. Para ello, se necesitara saber cuál es la información y en donde se encuentra para que pueda proceder a definir los controles que se necesitan para protegerla.

## INDICE DE CUADROS Y FIGURAS

## REFERENCIAS BIBLIOGRAFICAS


Barman, Scott

2002 Writing Information Security Policies
2002 New Riders Publishing

CERT

2007 http://www.cert.org/

Hansteen, Peter N. M.

2007 The Silent Network - Denying the Spam and Malware Chatter using Free Tools

IBM Internet Security Systems X-Force®

2007 IBM Internet Security Systems X-Force® 2006 Trend Statistics
January 2007
© Copyright 2007, IBM

INTERNATIONAL STANDARD - ISO/IEC JTC 1/SC 27

2005 ISO/IEC FDIS 17799: 2005-02-11 — Information techniques — Security techniques — Code of practice for information security management (2nd edition)

Izquierdo Duarte, Fernando

2003 Administración de Riesgos de Riesgos de TI: Manizales, Colombia

Peltier, Thomas R.

1999 INFORMATION SECURITY - POLICIES and PROCEDURES
A Practitioner's Reference
CRC Press LLC

Tipton, Harold F. y Krause, Micki

2007 Information Security Management Handbook
Sixth edition: Auerbach Publications

Universidad Autónoma De México
2007 UNAM CERT
http://www.cert.org.mx/

Universidad Nacional de Colombia
2007 Dirección Nacional de Informática y Comunicaciones (Dnic )
Seguridad Informática
http://www.unal.edu.co/seguridad/index.html

Warkentin, Merrill y Vaughn, Rayford B.
2006 Enterprise Information Systems
Assurance and System Security: Managerial and Technical Issues

Wikipedia, la enciclopedia libre
2007 http://es.wikipedia.org/wiki/Portada